# DualCard User Manual

**DUALi Inc.**

Document Version: 1.02

Last Revised Date: 30 April 2010

Copyright ⓒ 2009 DUALi Inc. All rights reserved. You are strictly prohibited to copy, disclose, distribute, or use this document in part or as a whole for any purposes other than those for which this document is disclosed. This document is copyrighted and contains confidential information and other intellectual property rights of DUALi Inc. Any unauthorized use, copy, disclosure or distribution constitutes infringement of DUALi's intellectual property rights.

Secure yet convenient
www.duali.com

DUALi Inc. reserves the right to make changes to its applications or services or to discontinue any application or service at any time without notice. DUALi provides customer assistance in various technical areas, but does not have full access to data concerning the use and applications of customer's products.

Therefore, DUALi assumes no liability and is not responsible for customer applications or software design or performance relating to systems or applications incorporating DUALi products. In addition, DUALi assumes no liability and is not responsible for infringement of patents and/or any other intellectual or industrial property rights of third parties, which may result from assistance provided by DUALi.

Composition of the information in this manual has been done to the best of our knowledge. DUALi does not guarantee the correctness and completeness of the details given in this manual and may not be held liable for damages ensuing from incorrect or incomplete information. Since, despite all our efforts, errors may not be completely avoided, we are always grateful for your useful tips.
We have our development center in South Korea to provide technical support. For any technical assistance can contact our technical support team as below;

Tel: +82 31 213 0074
e-mail : yekwon@duali.com

# Revision History

- 2009.02. (Ver. 1.0) : First Release
- 2009.05. (Ver. 1.01) : 15693(Optional. DE-620R) Function Added
- 2010.04. (Ver. 1.02) : Mifare plus function tap added

# CONTENTS

**INTRODUCTION** ..... **5**

**1. MAIN** ..... **6**

1.1 CONNECT ..... 6
1.2 TAB ..... 7
1.3 COMMAND INPUT ..... 7
1.4 PACKET LIST ..... 8

**2. 7816** ..... **11**

2.1 POWER ON, OFF ..... 11
2.2 COMMAND ..... 12

**3. 14443** ..... **13**

3.1 TYPE A ..... 13
3.2 TYPE B ..... 15
3.3 SIMPLE CARD COMMAND ..... 16
3.4 COMMON FUNCTION ..... 16

**4. MIFARE** ..... **19**

4.1 MIFARE ..... 20

**5. MIFAREPLUS** ..... **22**

5.1 ACTIVATION ..... 23
5.2 AES128 ..... 24
5.3 AUTHENTICATION ..... 24

**6. FELICA** ..... **26**

6.1 OPEN & MUTUAL AUTHENTICATION WITH RW-SAM ..... 26
6.2 ID & PARAMETER ..... 27
6.3 FELICA CARD ACCESS COMMAND & DATA ..... 28

**7. DESFIRE** ..... **30**

7.1 DESFIRE ..... 30

**8. PCSC ..... 36**

8.1 CONNECT & DISCONNECT ..... 36
8.2 TRANSACTION ..... 37

**9. 15693 (OPTIONAL – DE-620R) ..... 38**

9.1 INVENTORY & SELECT ..... 38
9.2 READ / WRITE ..... 39
9.3 FLAG SELECTION, CREATE COMMAND AND EXECUTION ..... 39

**10. NFC ..... 41**

10.1 SET COMMUNICATION MODE ..... 42

**11. UTIL ..... 43**

11.1 SERIAL COMMUNICATION TEST ..... 43
11.2 CONVERSION ..... 44
11.3 CHANGE MODE ..... 44

**12. ANNEX ..... 46**

12.1 MIFARE COMMAND ..... 46
12.2 FELICA COMMAND ..... 47
12.3 DESFIRE COMMAND ..... 48

**13. EXAMPLE ..... 50**

13.1 ADD COMMAND TO PACKET LIST AND SAVE/LOAD COMMAND SET ..... 50
13.2 MIFARE ..... 52
13.3 FELICA ..... 55
13.4 DESFIRE ..... 58
13.5 PCSC ..... 61

# Introduction

## A. Intended Readership

This manual has been written keeping in mind the end-user, who uses the application and which mainly acts as a reference manual.

## B. Purpose

This manual contains information for establishing your work using this software. It describes the various functions that will be provided in the application. The purpose of this document is to give detail description about the Application Controls, Interface with Reader and Card.

## C. Scope

DUALi DualCard Application Supports DE-620 Reader which in return support wide range of Tags Compliant with ISO 7816, ISO 14443 Part 3 & 4 TYPE A/B, Mifare, FeliCa, DesFire Standards

Application of DualCard are:-

- Card Test Solution.
- DUALi Reader Test Solution.

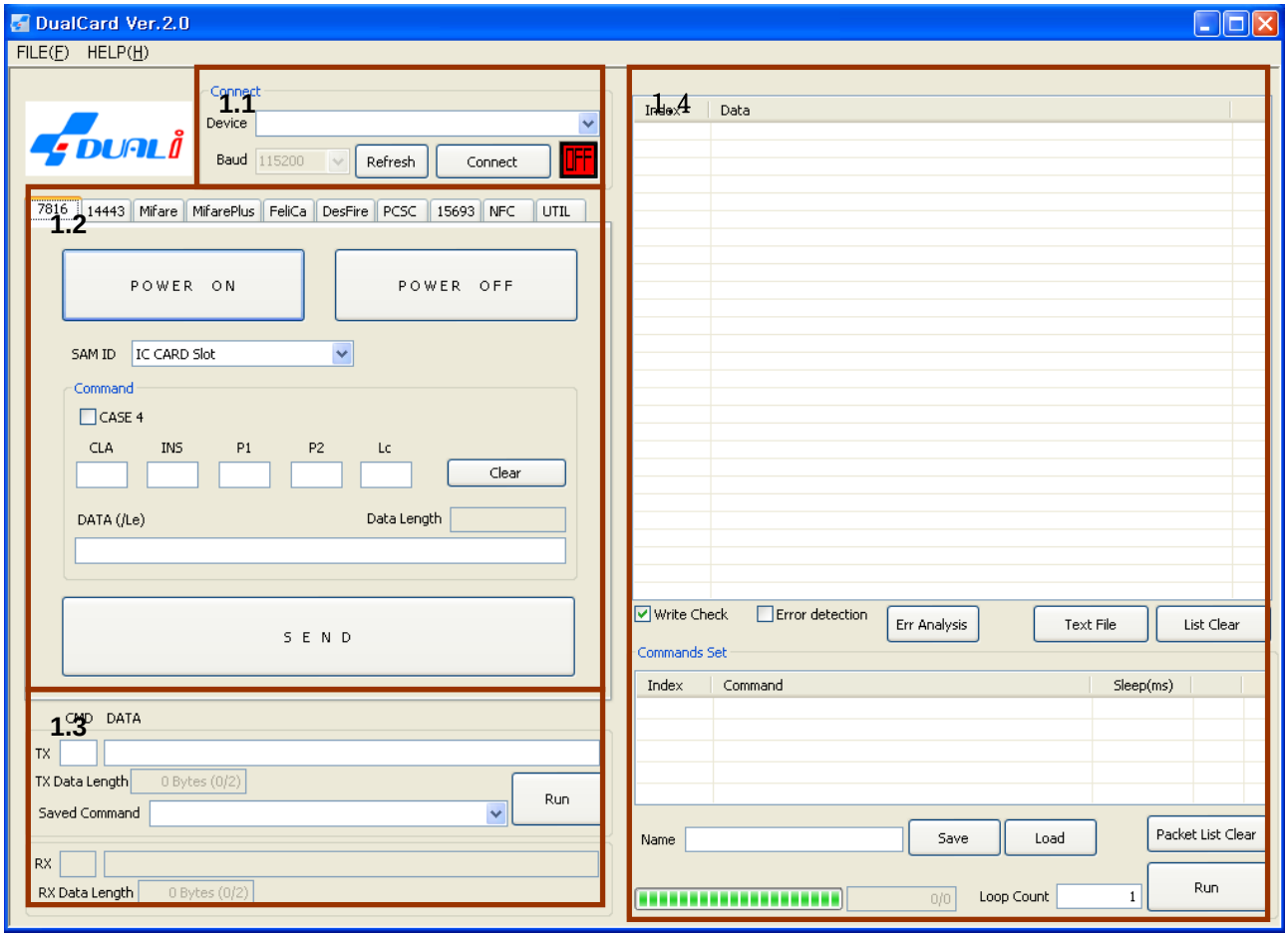
FeliCa is registered trademark of SONY corporation

Mifare and DesFire are registered trademarks of NXP Semiconductors

Supportive O/S

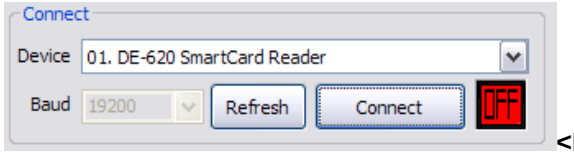
Windows 2000, Windows XP, Windows Vista (32bit), Windows 7 (32bit)

# 1. Main




**< Figure 1-1 > The Main function of DualCard program.**

## 1.1 Connect



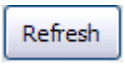

**<Figure 1-2>**

**It shows the list of currently connected RF module/device of DUALi (via USB or Hyper Terminal(RS-232))**

**And User can select & connect with the reader.**

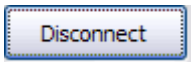
**(In case of using UART, standard communication speed set as 115200bps)**

- Select reader from Device list and click button to connect with the selected reader.

- While program runs, when additional reader is connected, click 

button to add additional reader to the Device list.

- If device is connected, [Connect] button in <Figure 1-2> will be change to


- If device is disconnected, 

button return back to <Figure 1-2>

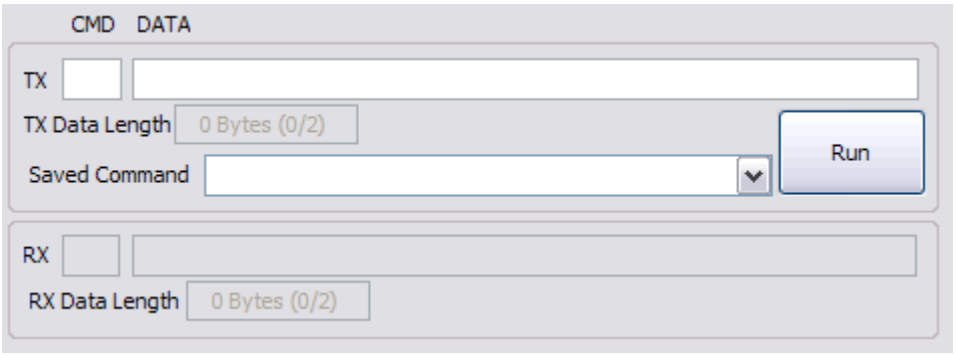
## 1.2 Tab

**<Figure 1-3>**

**This Tap shows various supportive card types and provide User useful test environment**

- It displays ISO 7816, ISO14443 A/B, Mifare, MifarePlus, FeliCa, DesFire, PCSC, ISO15693, NFC and Utility functions, you can select one.

## 1.3 Command input

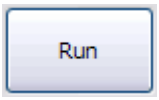



**<Figure 1-4>**

**This part for User input direct command from Protocol spec and send it to connected device**

**Each command has to be 1 byte Command code and data (as Hexadecimal)**

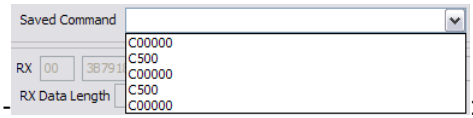
-

: Input the command (2 digit Hexadecimal) at 1st block , User data to 2nd block and click 

button to execute command.

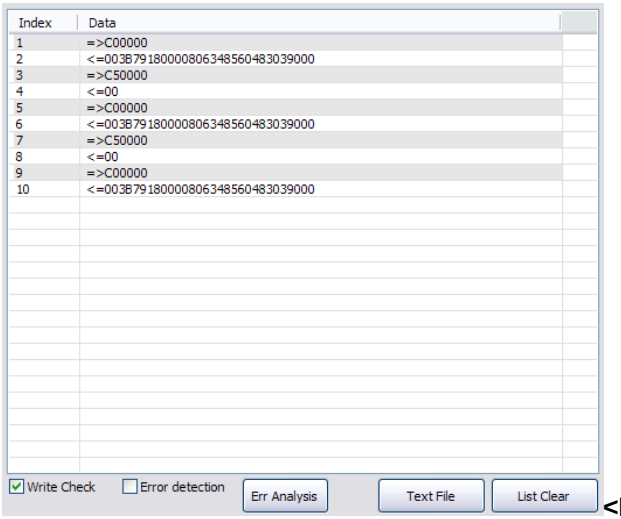
-

: it displays response from reader/card, Response code displays at 1st block, response data displays at 2nd block.



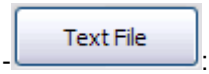
- : It shows saved commands up to 10 in orders of last executed .

## 1.4 Packet list



**<Figure 1-5>**

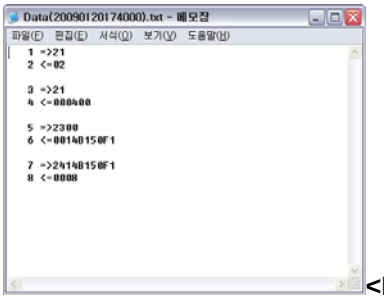
**This park displays Commands and Response Lists, it shows all communication data between PC and Device**. **Double-click on command; you can add command to packet list of <Figure 1-8>**



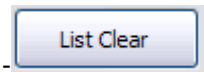
- : This button is for making lists of commands and responses <Figure 1-5> as text format file as <Figure 1-6>. The file name generated automatically following year, month, date as following e.g.

E.g) Data(20081222140537).txt

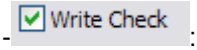
If you save file, it will be saved in 'DualCard\text' folder.



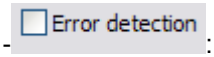
**<Figure 1-6>**



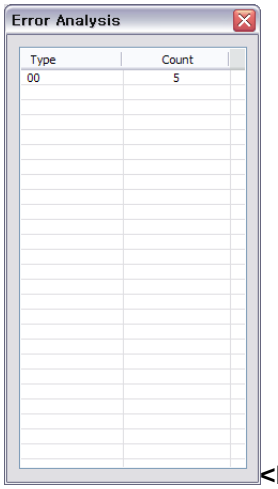
- : Delete all the commands and responses in the List.



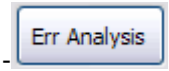
- : If you check this box, all communication data(Commands & Responses) will be shown at Packet list and it it's not checked, the command and response <Figure 1-5> will be not shown on the list.

- 

: This box is for Loop testing, If this box is checked it'll be stopped when Response code is Error code.



**<Figure 1-7>**

- 

: Click this icon to see error information.

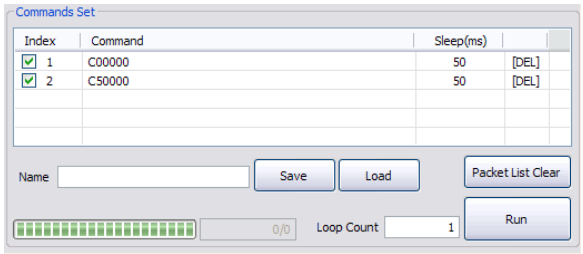
- Error information

**00 : No Error**

**02 : No response from the card.**

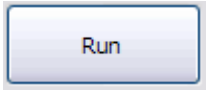
**03 : CRC Error**

**17 : Unknown command**

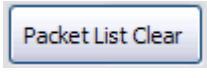


**<Figure 1-8>**

- Double click a command from list <Figure 1-5>, selected command will be added to packet list <Figure 1-8>.

- Press 

to execute command as loop count value. Commands of checked box in the Index field will run.

- Double click '[DEL]' in list <Figure 1-8> to delete selected command. Press 

to clear the list.

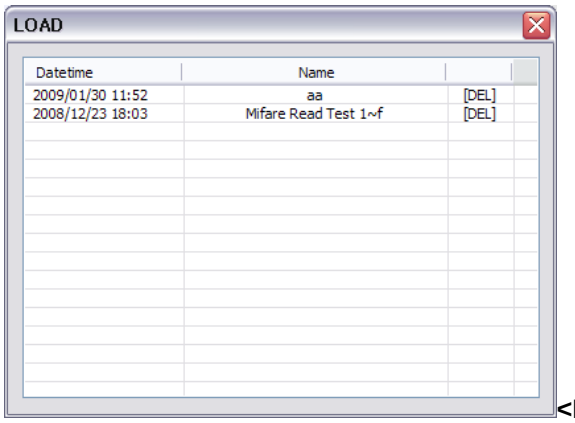
- To save command list as a file, Input file name in

and click

Save button. It'll be saved in packet list to DB.

- To bring saved file to the program, Click Load .

Selected file will be displayed as <Figure 1-9>




**<Figure 1-9>**

- To bring saved file to the program, Click Load and select file from the list <Figure 1-9>

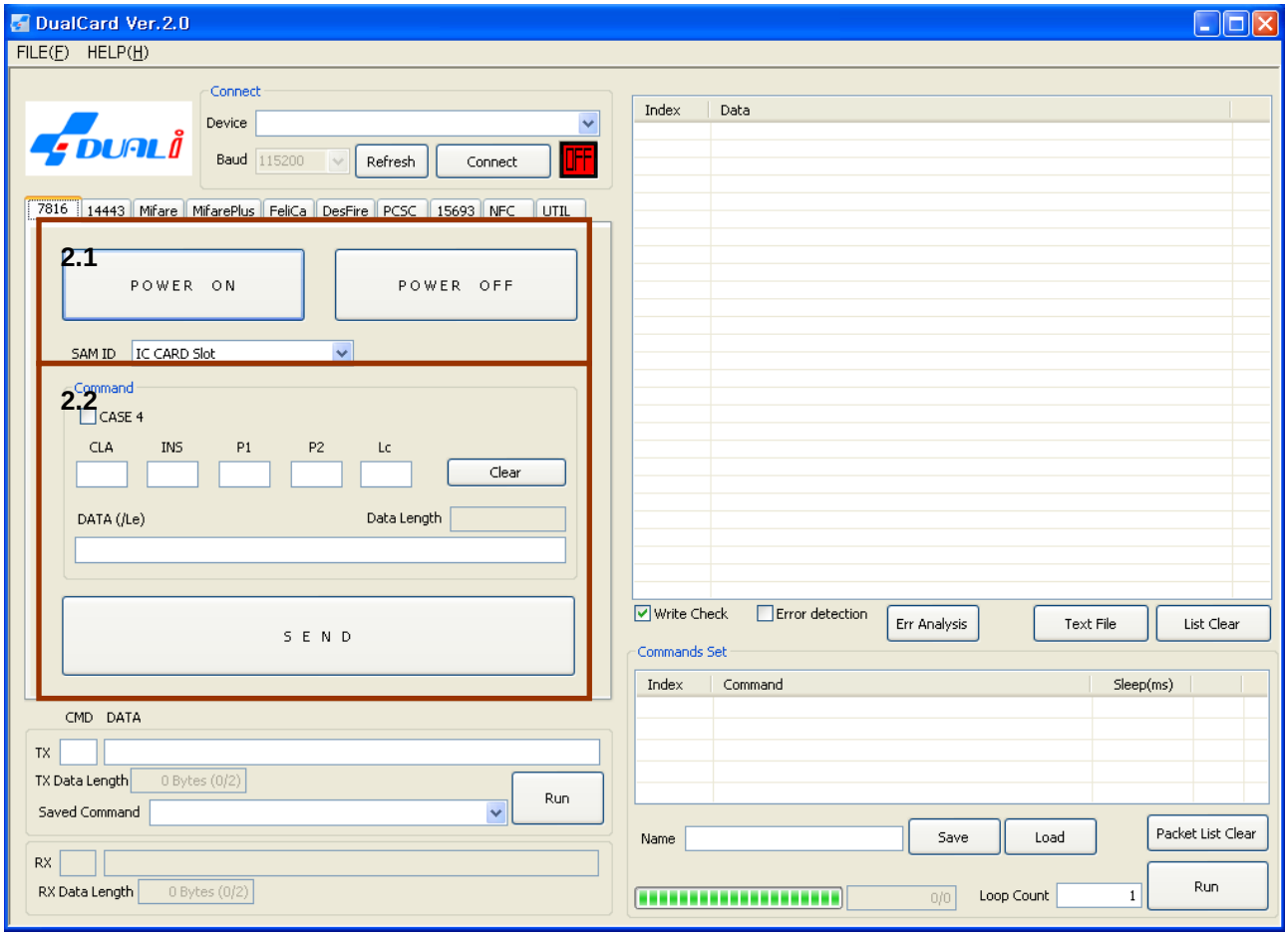
Double click on command set name in name field to add command set to packet list <Figure 1-7>.

- To delete Command Set, double click '[DEL]' next the file name from <Figure 1-9>'

# 2. 7816

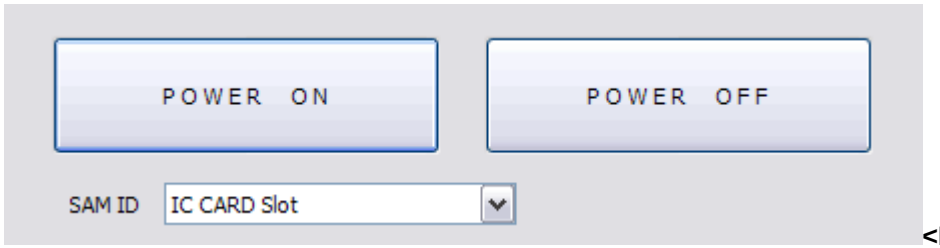
**This tap <Figure 2-1>supports Communication with ISO 7816 cards.**

**It is comprised of Power ON/OFF function part and Command execution part following ISO 7816.**



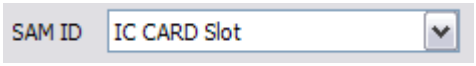

**<Figure 2-1>**

## 2.1 Power On, Off

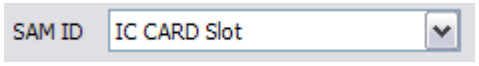



**<Figure 2-2>**

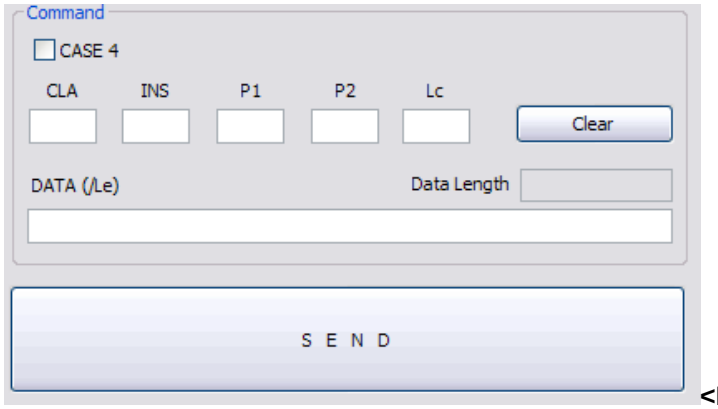
-

: This button is Power On command of Card slot ( SAM Slot/ IC Card Slot) which was selected from 

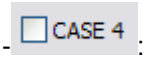
-

: This button is Power Off command of Card slot ( SAM Slot/ IC Card Slot) which was selected from 


## 2.2 Command



**<Figure 2-3>**

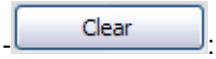
- 

: Check this box to execute command at Case 4.

-

: Input the command (2 digit Hexadecimal) as IC Card command format and press

button to execute command. Then response will be shown at the List.

- 

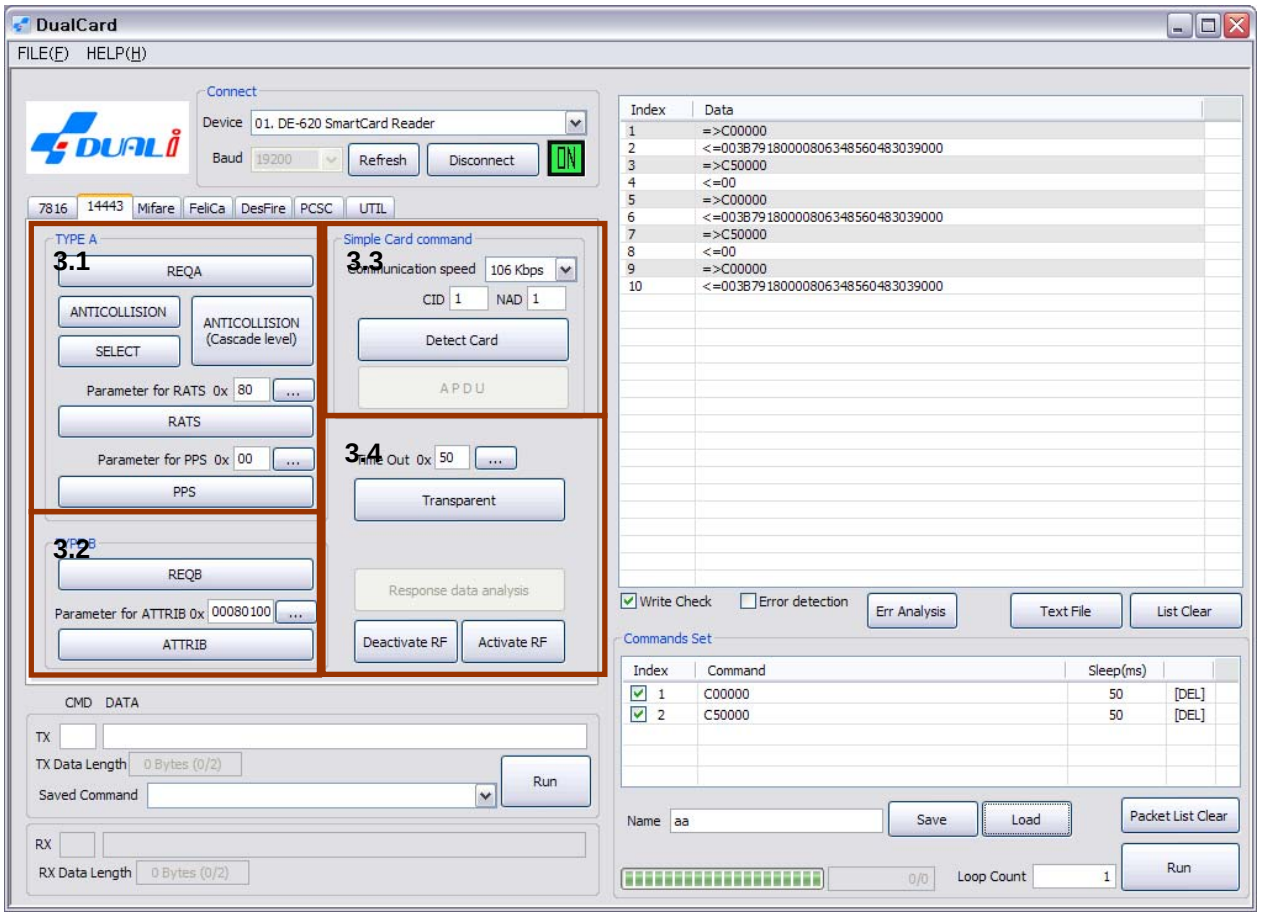
: Press this button to clear CLA, INS, P1, P2, LC, DATA(/Le).

# 3. 14443

**This tap <Figure 3-1>supports Communication with ISO 14443 A/B type cards.**

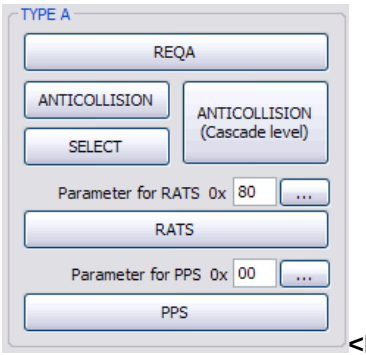
**It comprised of Type A Command set part, Type B Command set part, Card detect function part, User command transmit part and RF field control part.**

**Technical detail of protocol, refer to ISO 14443 Specification.**.

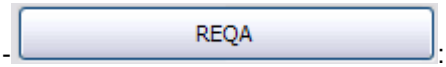



**<Figure 3-1>**

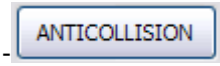
## 3.1 Type A



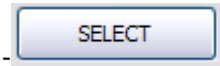

**<Figure 3-2>**

- 

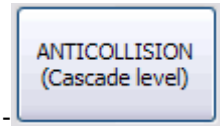
: To execute REQA command and get response.

- 

: To execute “Anti Collision(cascade level 1)” command and get response.

- 

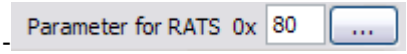
: To execute “Select” command and get response.

- 

: To execute “Anti Collision which supports cascade level” command and get response.

-

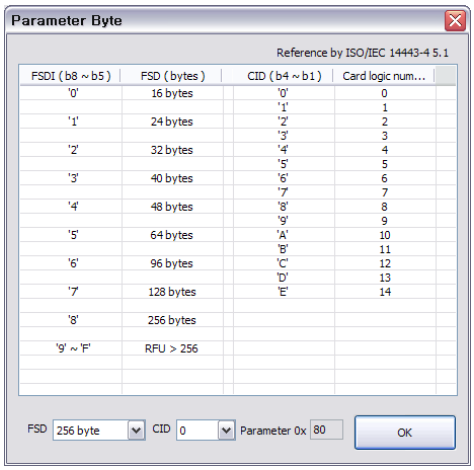
: To execute RATS Command and get response.

- 

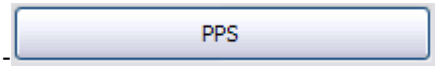
: Show Parameter byte for RATS.

-

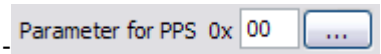
: Press this button shows parameter byte setting window for RATS. <Figure 3-3>



**<Figure 3-3>**

- 

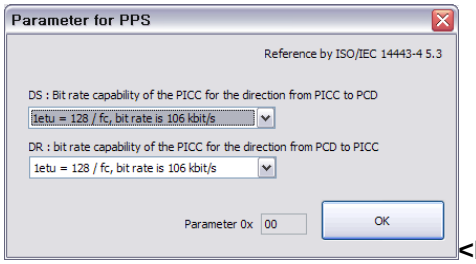
: To execute PPS Command and get response.

- 

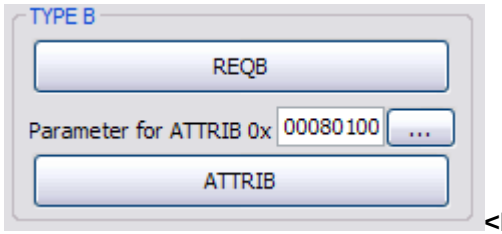
: Parameter byte for PPS

-

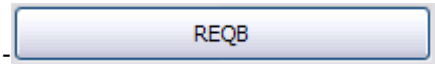
: Press this button shows parameter byte setting window for PPS.<Figure 3-4>.


Parameter for PPS
Reference by ISO/IEC 14443-4 5.3
DS : Bit rate capability of the PICC for the direction from PICC to PCD
1etu = 128 / fc, bit rate is 106 kbit/s
DR : bit rate capability of the PICC for the direction from PCD to PICC
1etu = 128 / fc, bit rate is 106 kbit/s
Parameter 0x 00
OK
**<Figure 3-4>**

## 3.2 Type B



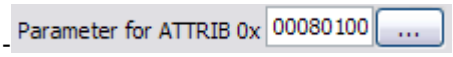

**<Figure 3-5>**

- 

: To execute “REQB” command and get response.

-

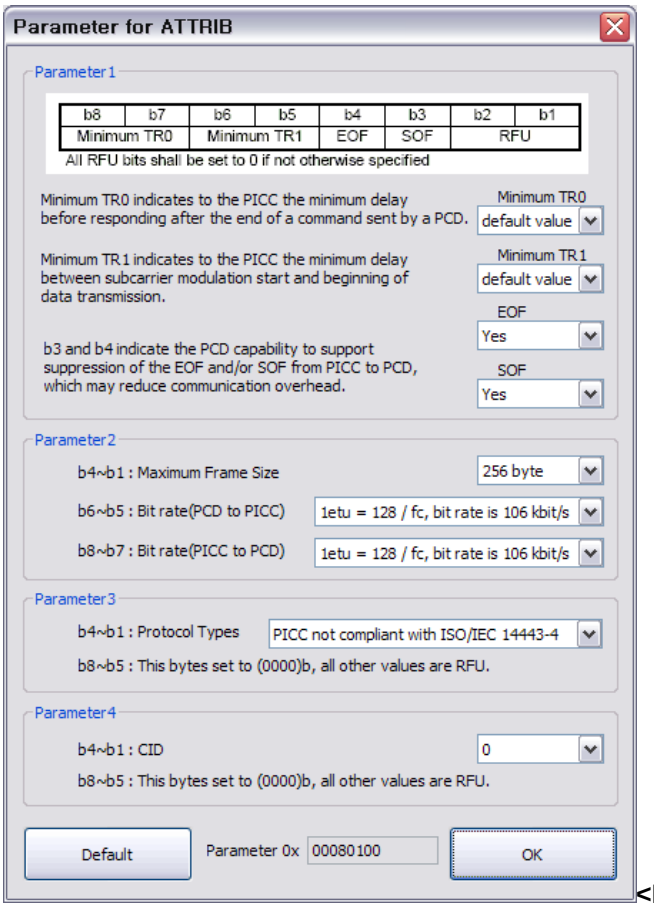
: To execute “ATTRIB” command and get response.

- 

: Parameter byte for ATTRIB.

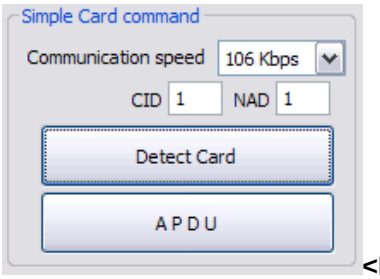
-

: Press this button shows parameter byte setting window for ATTRIB<Figure 3-6>

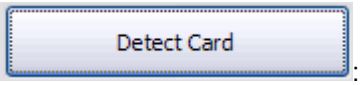

Parameter for ATTRIB
Parameter1
b8 b7 b6 b5 b4 b3 b2 b1
Minimum TR0 Minimum TR1 EOF SOF RFU
All RFU bits shall be set to 0 if not otherwise specified
Minimum TR0 indicates to the PICC the minimum delay before responding after the end of a command sent by a PCD.
Minimum TR0
default value
Minimum TR1 indicates to the PICC the minimum delay between subcarrier modulation start and beginning of data transmission.
Minimum TR1
default value
b3 and b4 indicate the PCD capability to support suppression of the EOF and/or SOF from PICC to PCD, which may reduce communication overhead.
EOF
Yes
SOF
Yes
Parameter2
b4~b1 : Maximum Frame Size
256 byte
b6~b5 : Bit rate(PCD to PICC)
1etu = 128 / fc, bit rate is 106 kbit/s
b8~b7 : Bit rate(PICC to PCD)
1etu = 128 / fc, bit rate is 106 kbit/s
Parameter3
b4~b1 : Protocol Types
PICC not compliant with ISO/IEC 14443-4
b8~b5 : This bytes set to (0000)b, all other values are RFU.
Parameter4
b4~b1 : CID
0
b8~b5 : This bytes set to (0000)b, all other values are RFU.
Default
Parameter 0x
00080100
OK

**<Figure 3-6>**

## 3.3 Simple card command




**<Figure 3-7>**

- 

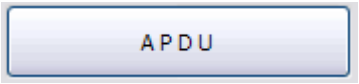
: To execute Detect Card command.

-

: Change communication speed as 106/212/424/848kbps

-

: To set CID and NAD value for card communication.

- 

: To add automatically PCB, CID from user's command which was input <Figure 1-4>

TX and execute this command.

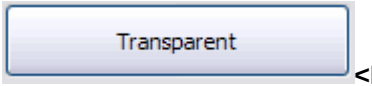
## 3.4 Common function

**<Figure 3-8>**

It defines the waiting time from device send command and get response.

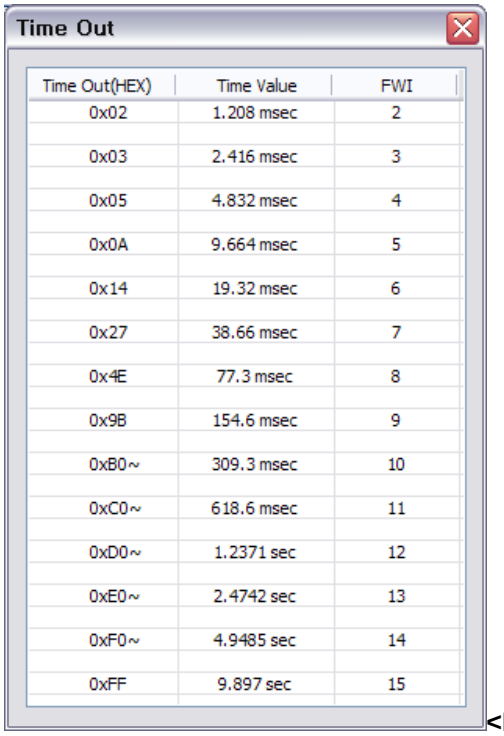
-

Press this button shows Time-our windows as <Figure 3-10> following time out box setting.




**<Figure 3-9>**

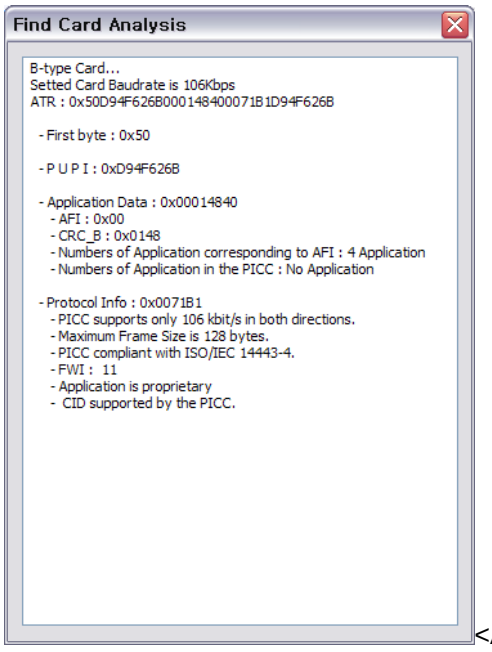
- To transmit defined command from the protocol (PC and Device) spec or APDU type command comply with ISO 14443 spec. You should input PCB, CID and NAD according to your card specification.




**<Figure 3-10> Actual waiting time following Time-out setting.**

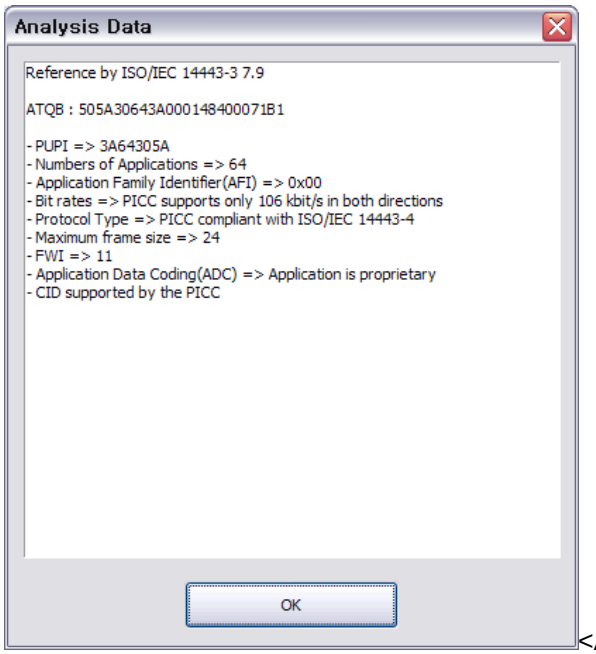
- Response data analysis : After execute [REQA] / [Anti-collision] / [Select] / [RATS] /[REQB] or [Detect Card] command, Press Response data analysis will show the response data analysis window as <Figure 3-11><Figure 3-12> .

- Deactivate RF, Activate RF : Activate or Deactivate RF field.


Find Card Analysis
B-type Card...
Setted Card Baudrate is 106Kbps
ATR : 0x50D94F626B000148400071B1D94F626B
- First byte : 0x50
- P U P I : 0xD94F626B
- Application Data : 0x00014840
- AFI : 0x00
- CRC_B : 0x0148
- Numbers of Application corresponding to AFI : 4 Application
- Numbers of Application in the PICC : No Application
- Protocol Info : 0x0071B1
- PICC supports only 106 kbit/s in both directions.
- Maximum Frame Size is 128 bytes.
- PICC compliant with ISO/IEC 14443-4.
- FWI : 11
- Application is proprietary
- CID supported by the PICC.

<Analysis for [Detect Card]>

**<Figure 3-11>**


Analysis Data
Reference by ISO/IEC 14443-3 7.9
ATQB : 505A30643A000148400071B1
- PUPI => 3A64305A
- Numbers of Applications => 64
- Application Family Identifier(AFI) => 0x00
- Bit rates => PICC supports only 106 kbit/s in both directions
- Protocol Type => PICC compliant with ISO/IEC 14443-4
- Maximum frame size => 24
- FWI => 11
- Application Data Coding(ADC) => Application is proprietary
- CID supported by the PICC
OK
<Analysis for A-type after RATS>

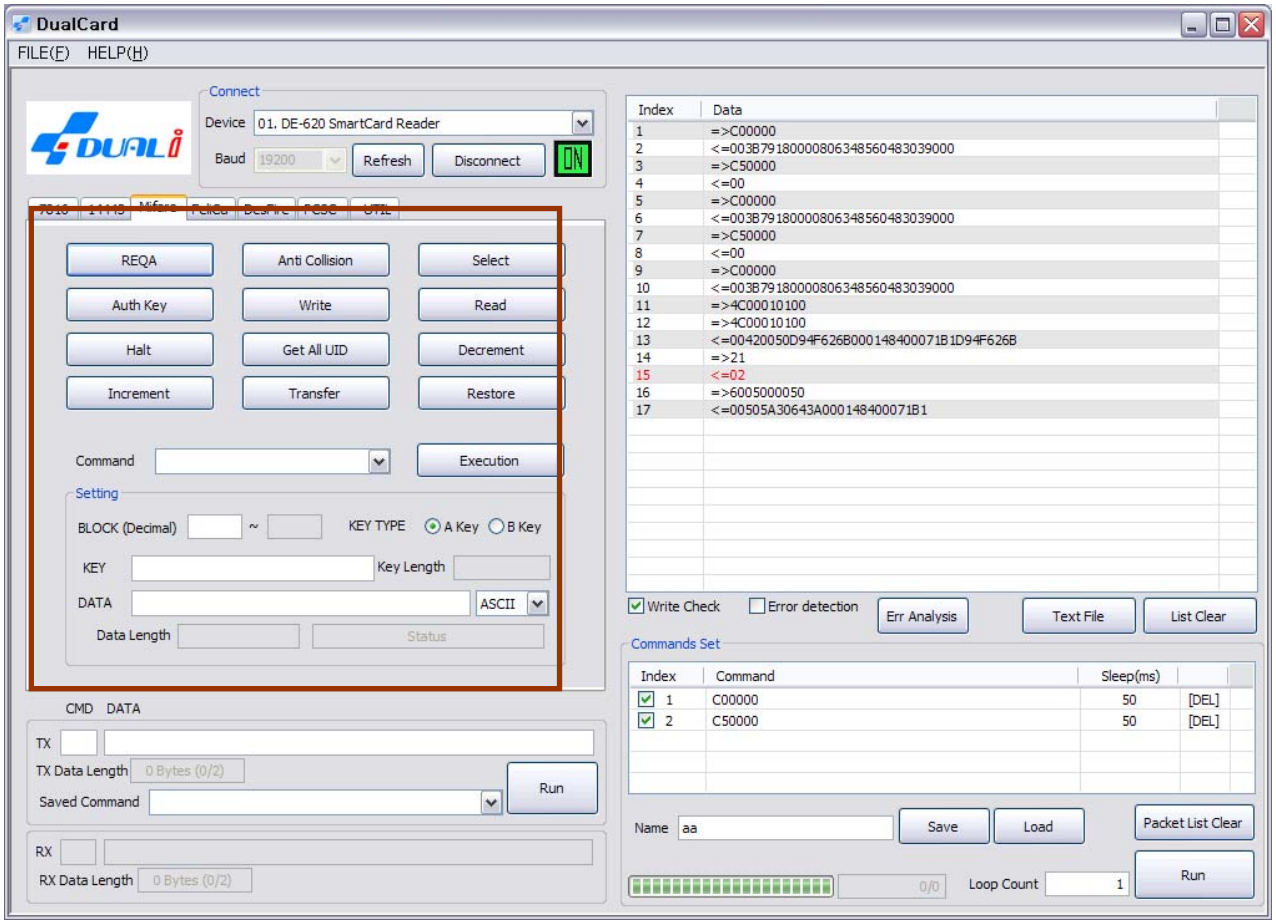
**<Figure 3-12>**

# 4. Mifare

**This tap <Figure 4-1>supports Communication with NXP's contactless memory card MIFARE protocol.**

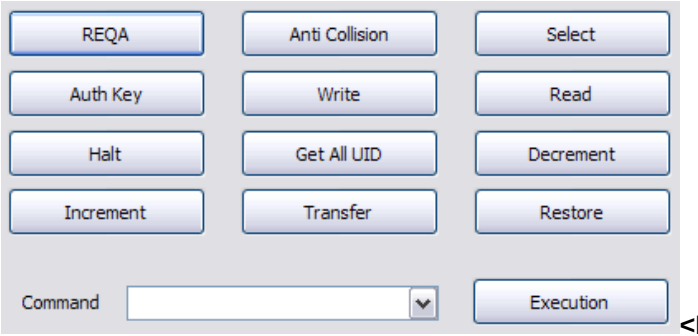
**It is able to check all functions of Mifare. Mifare cards (up to layer 2) use same protocol as ISO 14443 type A, and use their own protocol from layer 3.**

**It requires Authentication process to access memory of Mifare card. By providing 6 byte key gives permission to read/ write data inside memory. Each blocks are made of 16 byte, and the data process has to follow same 16byte format. Refer to NXP's Specification for detail technical information.**

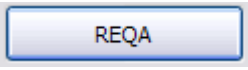



**<Figure 4-1>**

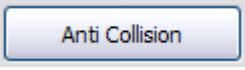
## 4.1 Mifare



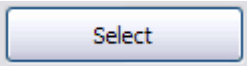

**<Figure 4-2>**

- 

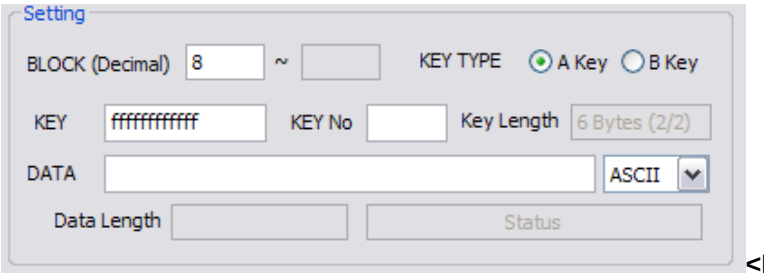
: To execute Request Command and get response.

- 

: To execute Anti Collision Command and get response.

- 

: To execute Select Command and get response.




**<Figure 4-3>**

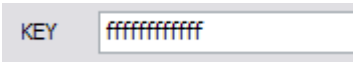
**This part shows Setting value for Authentication process**

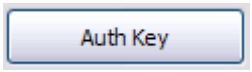
- Followings are Authentication process**.(See Example 13.2**)

1) Input block number to read


2) Select key type for using Authentication

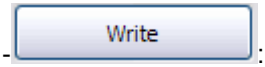
.

3) Input key value to access selected block (Hexadecimal, 6byte) 

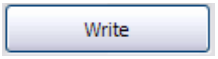

4) Press 

button will execute auth command and get response

- Following commands has to be executed after Authentication process above.

- 

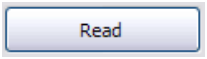
: To execute Write command. Input data

and press 

button.

-

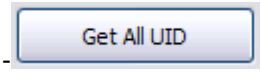
: To execute Read command, Input block number to read

and press 

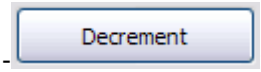
button. It'll show 16 bytes response when it succeed.

-

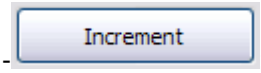
: To execute Halt command. After execute halt command, Mifare card doesn't response until it receive Wakeup Request.

- 

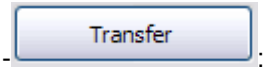
: To read the UID of all card in RF field. It'll be shown card's number which succeed Anti-collision process

- 

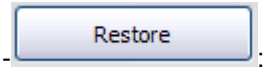
: To execute Decrement command for Value block. **(See Example 13.2)**

- 

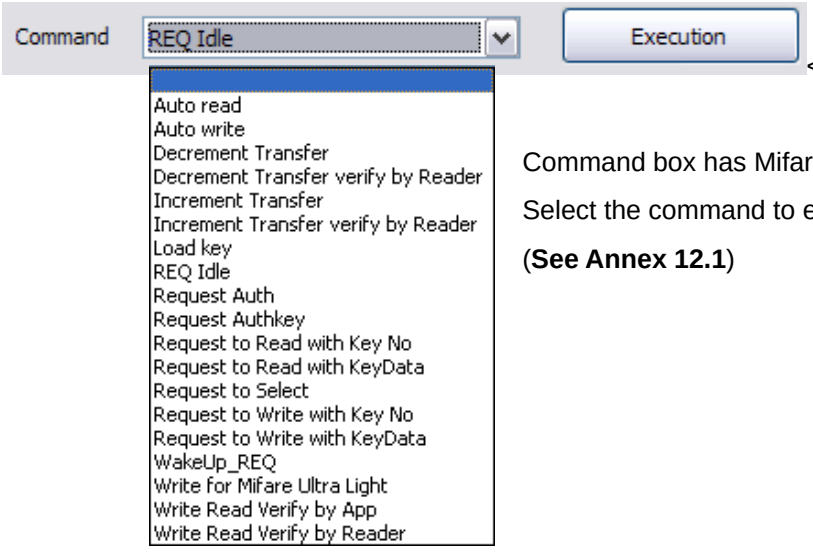
: To execute Increment command for Value block**. (See Example 13.2)**

- 

: To execute Transfer command for Value block.

- 

: To execute Restore command for Value block.



<Figure 4-4>

Command box has Mifare command list.

Select the command to execute and press Execution button.

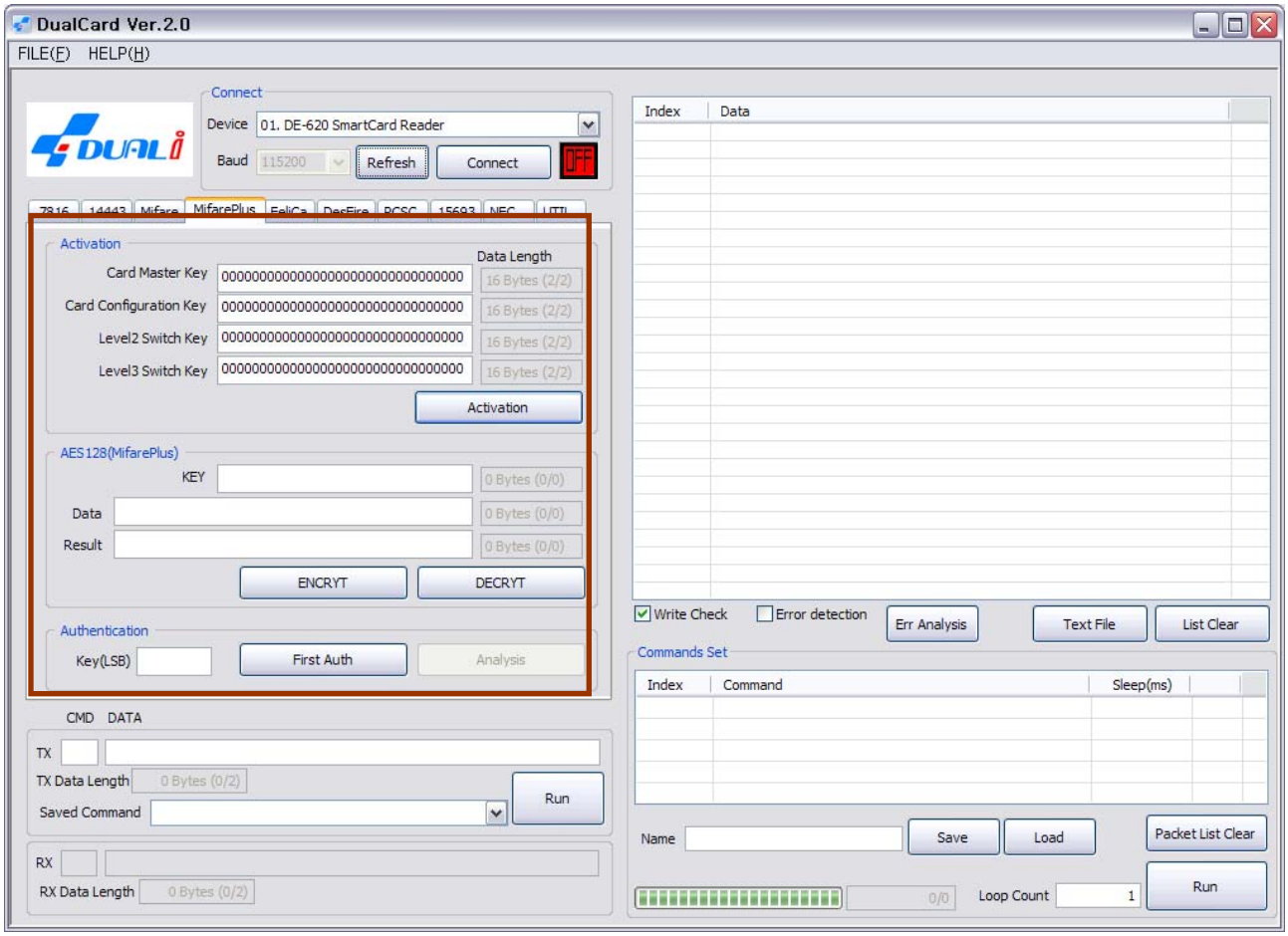
(**See Annex 12.1**)

# 5. MifarePlus

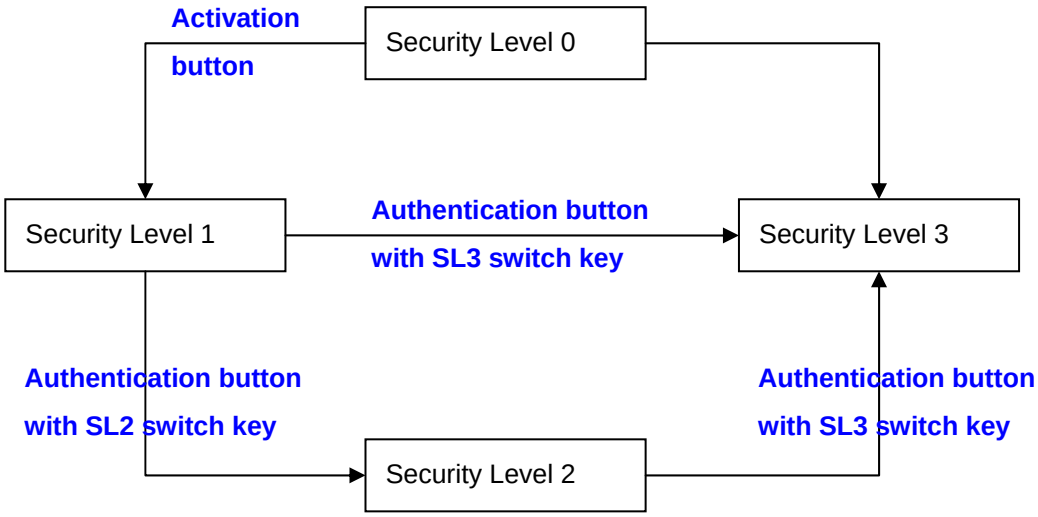
**This tap <Figure 5-1>supports Communication with NXP's next version of MIFARE card, MifarePlus.**

**MifarePlus is strengthen the security function compare with Mifare card, so it isn't response before Pre-personalization.**

**MifarePlus level 1 card is compatible with Mifare card completely, MifarePlus level 2 card use AES128 algorithm for Authentication process, MifarePlus level 3 card adopt ISO 14443 Type A –APDU format.**

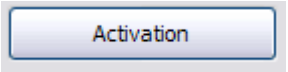



**<Figure 5-1 >**




**<Figure 5-2 Security level switching >**

## 5.1 Activation



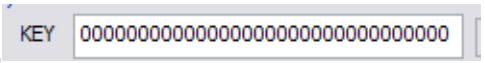

- This button uses for converting Security level 0(default)card to Security level 1 card (same as Mifare card). Level 1 card is compatible with Mifare card.
- Fill out each key (default =0000000…000000), press “Activation button”. It’ll process as following.
  - [REQA] -> [ANTICOLLISION] -> [SELECT] -> [RATS] -> [WRITE PERSO for each keys] -> [COMMIT PERSO]
- This Activation process, set [Card Master key]. [Card Configuration key], [Level 2 switch key], [Level 3 switch key] only which is mandatory to activate the card. Other keys can be changed after “Activation” process and “Authentication”.
- [Level 2 switch key] is a mandatory for Activation, but it can be skipped depend on card types. There are “x” & “s” version of MifarePlus cards, it doesn’t need for “s” version of cards because it doesn’t support Level 2.
  - **After “Activation” process, Mifare Plus card become Level 1 card (same as Mifare card). User can move to the “Mifare” tap for the next process (card read & write). Please refer to 4. Mifare tap Usage guide**

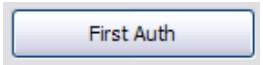
## 5.2 AES128

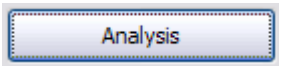
- MifarePlus cards use AES128 algorithm for authentication.
- AES 128 algorithm is necessary for Authentication, and communication with Level2, Level3 cards.
- Input [Key] and [Data], then press [ENCRYPT] button. It'll show the result in [Result] box after Data encryption using AES128 Algorithm.
- Input [Key] and [Data], then press [DECRYPT] button. . It'll show the result in [Result] box after Data decryption using AES128 Algorithm.

## 5.3 Authentication

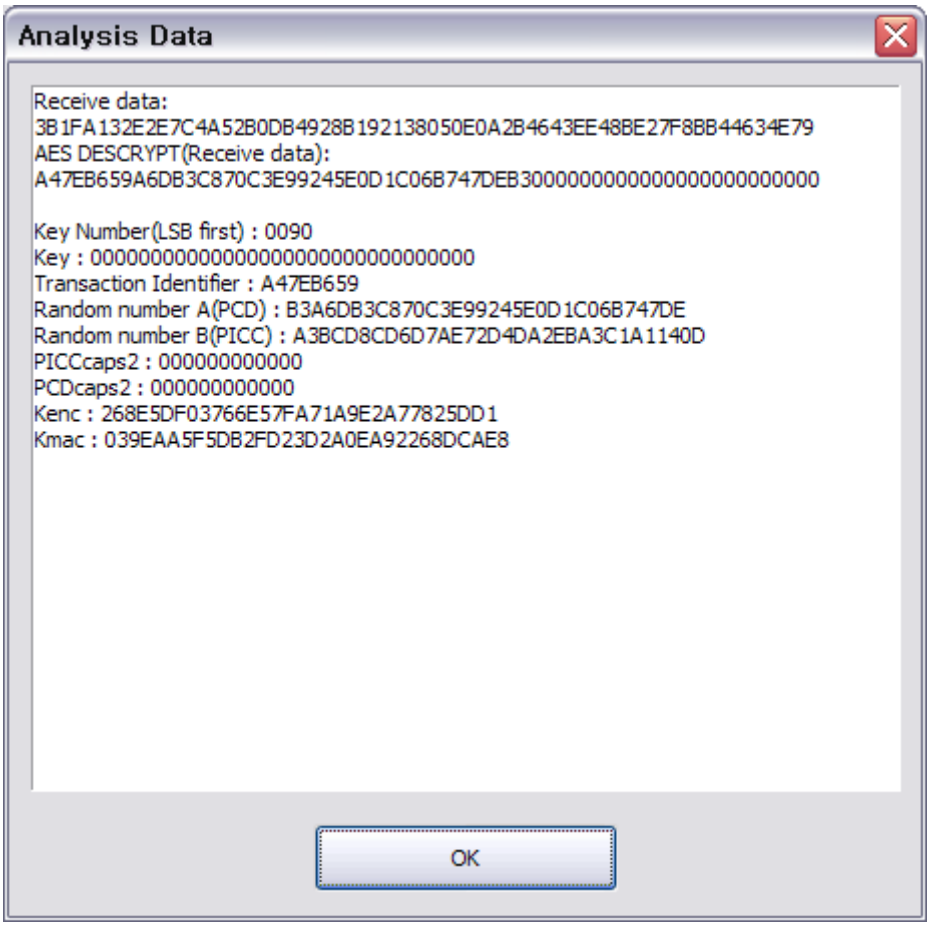
- Input the Key to Auth as following,


- Input the Key for selected Key(LSB) as following, 


- After input above two data, press 

button. It'll process Authentication.
- e.g] Place Level 3 card on DE-620, input Card master key into [Key]box, and input the key for selected key [0090]. When you press this (First Auth) button, it'll process Authentication for Card master key.
- When Authentication proceeds successfully, 

button becomes activated. Press this (Analysis) button; you'll see the Analysis Data as following.

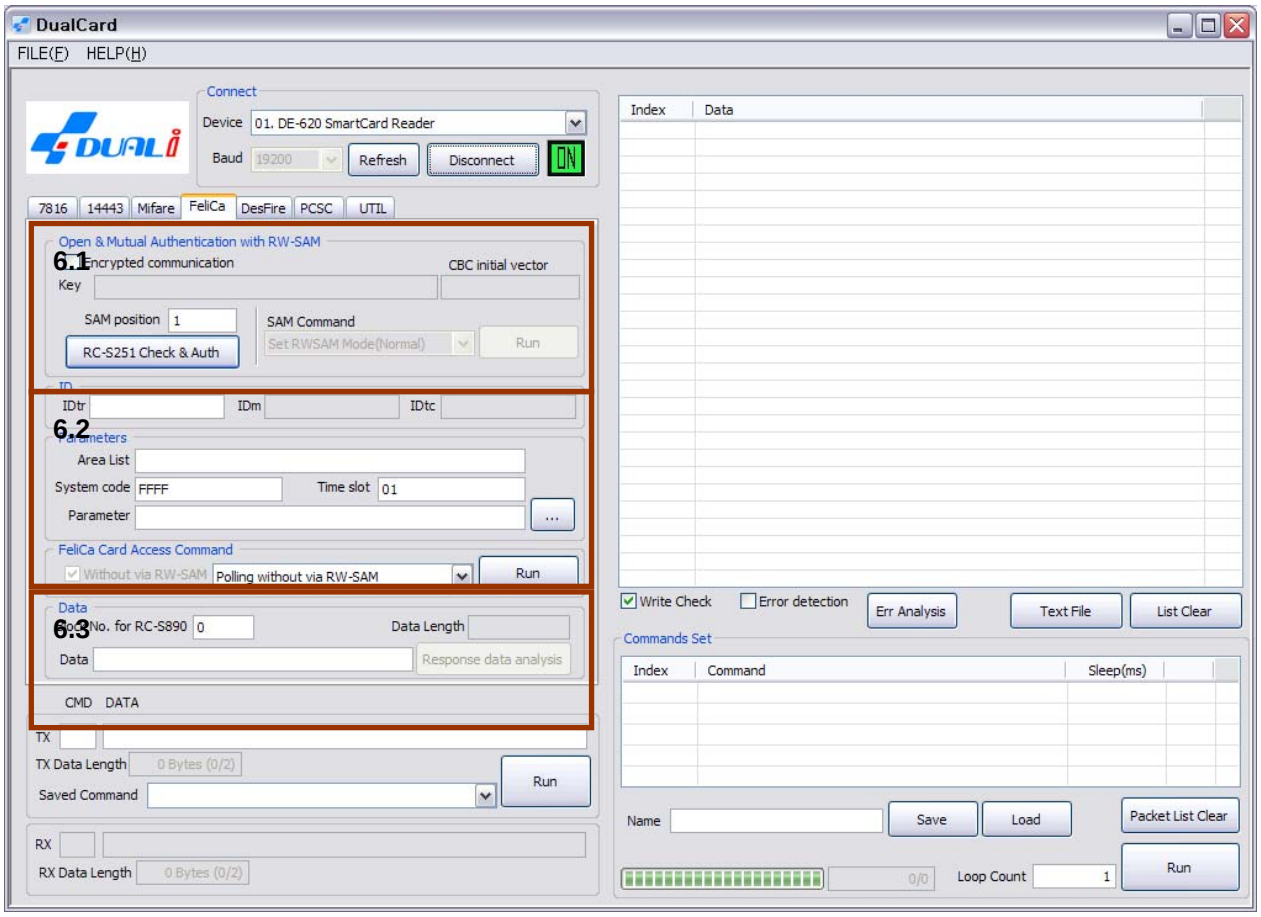

Analysis Data
Receive data:
3B1FA132E2E7C4A52B0DB4928B192138050E0A2B4643EE48BE27F8BB44634E79
AES DESCRYPT(Receive data):
A47EB659A6DB3C870C3E99245E0D1C06B747DEB300000000000000000000000000
Key Number(LSB first) : 0090
Key : 00000000000000000000000000000000
Transaction Identifier : A47EB659
Random number A(PCD) : B3A6DB3C870C3E99245E0D1C06B747DE
Random number B(PICC) : A3BCD8CD6D7AE72D4DA2EBA3C1A1140D
PICCcaps2 : 000000000000
PCDcaps2 : 000000000000
Kenc : 268E5DF03766E57FA71A9E2A77825DD1
Kmac : 039EAA5F5DB2FD23D2A0EA92268DCAE8
OK

# 6. FeliCa

**This tap <Figure 6-1>supports Communication with Sony's FeliCa card.**

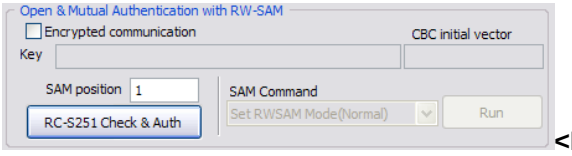
**It uses for RC-S251 RW-SAM card (SIM type) which allows higher security transacation.**

**This program based on SONY's sample 5 card for Secure logic & keys. Refer to Sony's FeliCa specification for detail technology information.**




**<Figure 6-1>**

## 6.1 Open & Mutual Authentication with RW-SAM

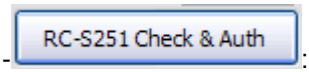



**<Figure 6-2>**

- Encrypted communication : Check this box in order to use encrypted communication with RC-S251 SAM.

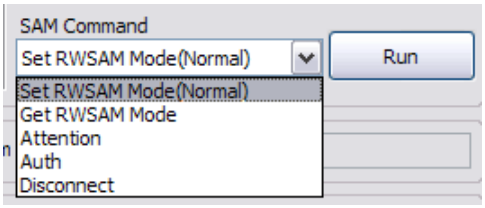
  (For encrypted communication, using RW-SAM is necessary)

- SAM position 1 : Select SAM slot position.

- 

:To execute mutual authentication with RC-S251 SAM and get result.

(Batch execution button for mutual authentication)



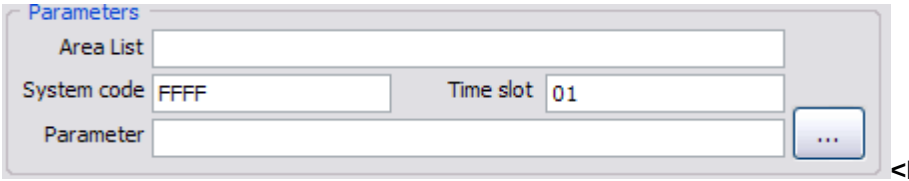
**<Figure 6-3>**

- Set RWSAM Mode(Normal) : Set RW/SAM for mutual authentication(first step of mutual authentication). Change RWSAM from neutral mode to normal mode.
- Get RWSAM Mode: To get current mode of RWSAM.(Second step of mutual authentication)
- Attention : To detecting RWSAM.(Third step of mutual authentication)
- Auth : To execute Authenticate1 and Authentication 2 command(Last step of mutual authentication)
- Disconnect : To allow RWSAM mode from Mode 2 to Mode 0.

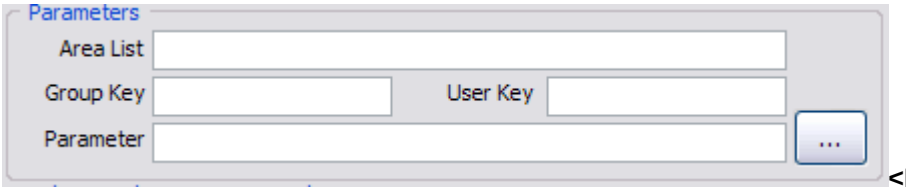
## 6.2 ID & Parameter

**<Figure 6-4>**

- IDtr(Transaction ID) : This value will be increase automatically whenever the card communicate with the RWSAM but you can change this value manually.
- IDm (Manufacture ID): Response value from card by Polling command.
- IDt(Card table ID): Response value from card by Mutual Authentication command.



**<Figure 6-5>**



**<Figure 6-6>**

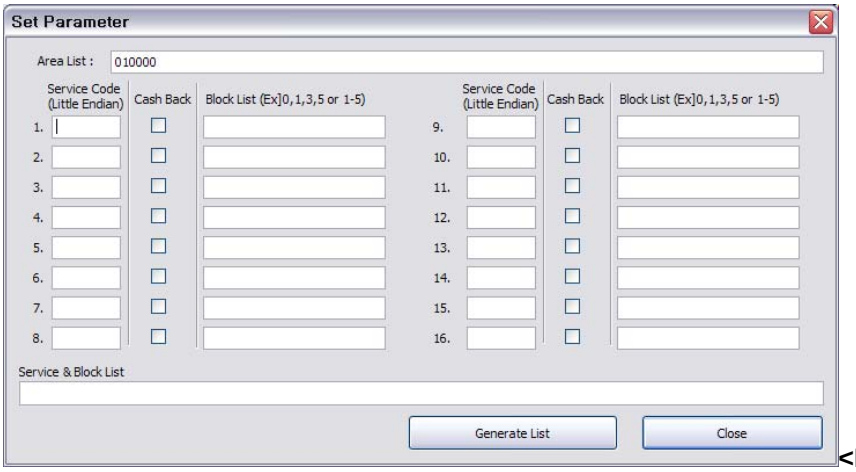
*** In case of sending Polling command. <Figure 6-5>**

- Area List : Don't use
- System code : Input 2 byte System code.
- Time slot : Set time slot value using for Polling command

*** In case of sending other command <Figure 6-6>**

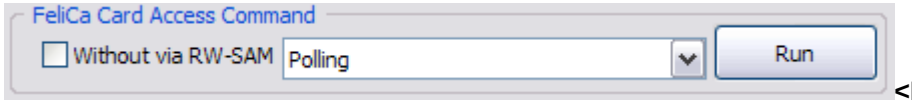
- Area List : Same as **<Figure 6-5>**
- Group key : .Input group key.
- User Key : Input User Key.
- Parameter : Input service & block list directly here. Also press

button to open window<Figure 6-7> for generate service & block list. After generate list, it will add to parameter box<Figure 6-5>. **<See Example 13-3>**

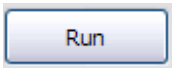


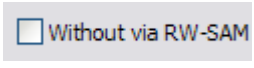
**<Figure 6-7>**

## 6.3 FeliCa Card Access Command & Data



**<Figure 6-8>**

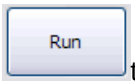
- Select Command from the list and click 

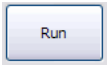
to execute selected command **(See Annex 12.2)**
- 

: Check this for execute command which doesn't need RW-SAM. When this box checked, Command list would change to command set which doesn't need security.

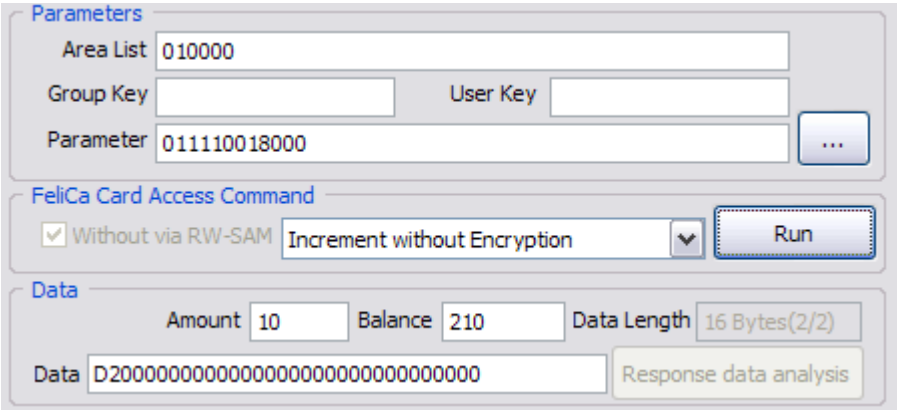
**<Figure 6-9>**

- ① Block No. for RC-S890 is for S890 (token type card) which doesn't need to generate Service & Block list (S890 is allowed to access only 1 block at one time)

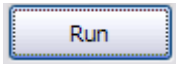
- Input data to write in ②DATA box and click 

to execute the command.
- It shows the reading data from card, when you select “Read command” in command list<Figure 6-3>, and click 

to execute command



**<Figure 6-10>**

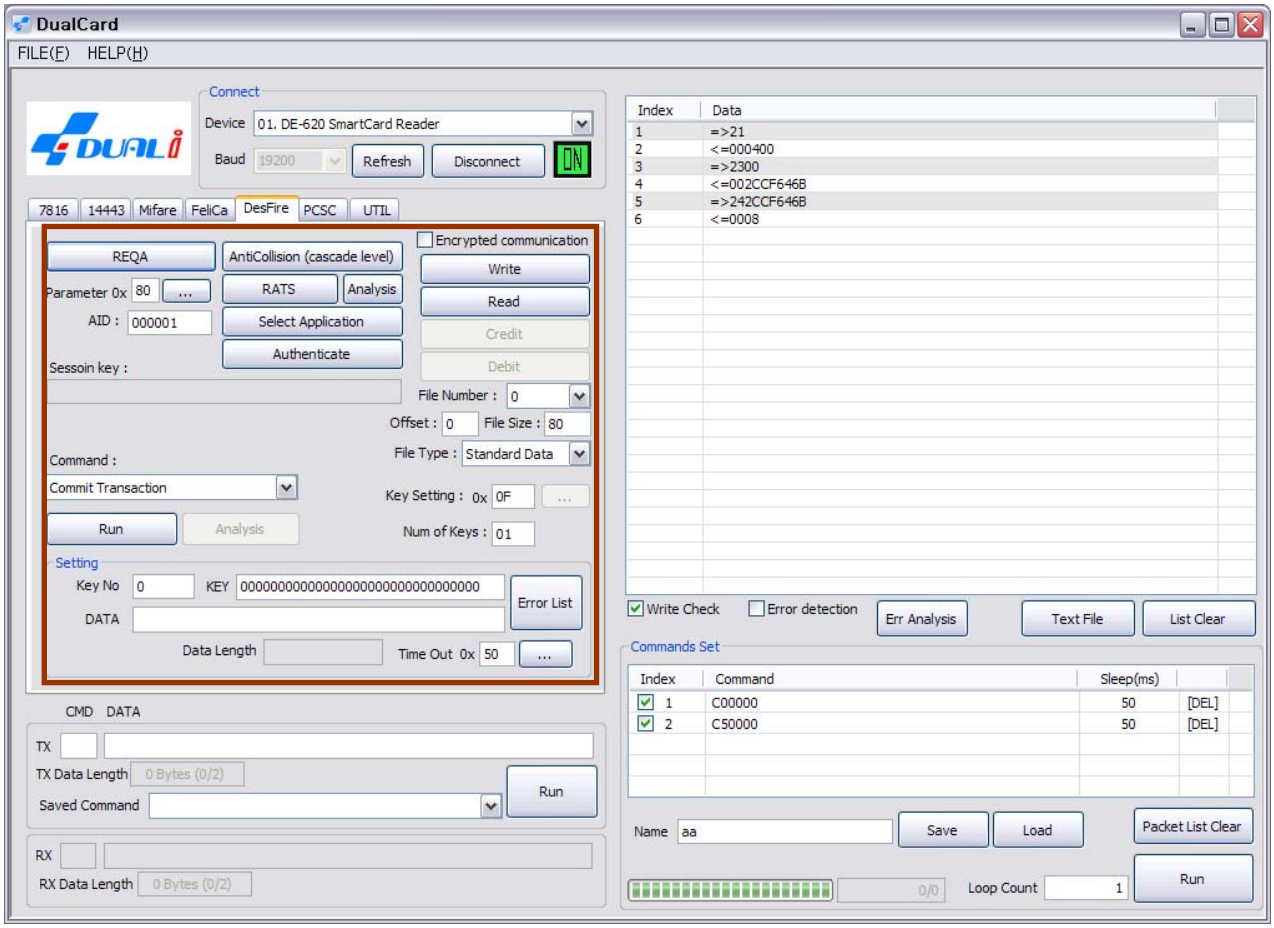
- In case of User select following command - “Increment without Encryption” , “Decrement without Encryption”, “Cashback without Encryption” and “Read Balance without Encryption”, <Figure 6-9> will change to <Figure 6-10>.
- In <Figure 6-10>, select command “Increment without Encryption” and input Area List & Parameter, then click 

button to execute the command, it’ll show balance of card.

# 7. DesFire

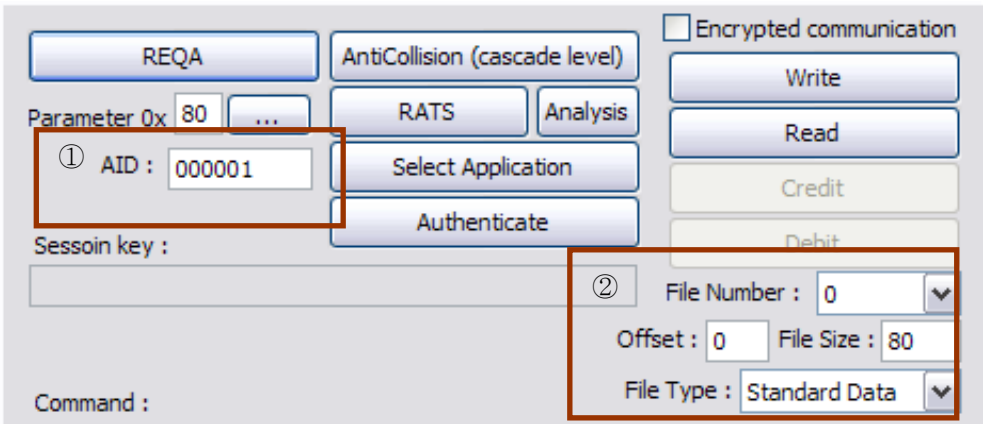
**This tap <Figure 7-1>supports Communication with NXP's DesFire card.**

**DesFire card is similar as Mifare card but strengthen security level using DES algorithm**




**<Figure 7-1>**

## 7.1 DesFire

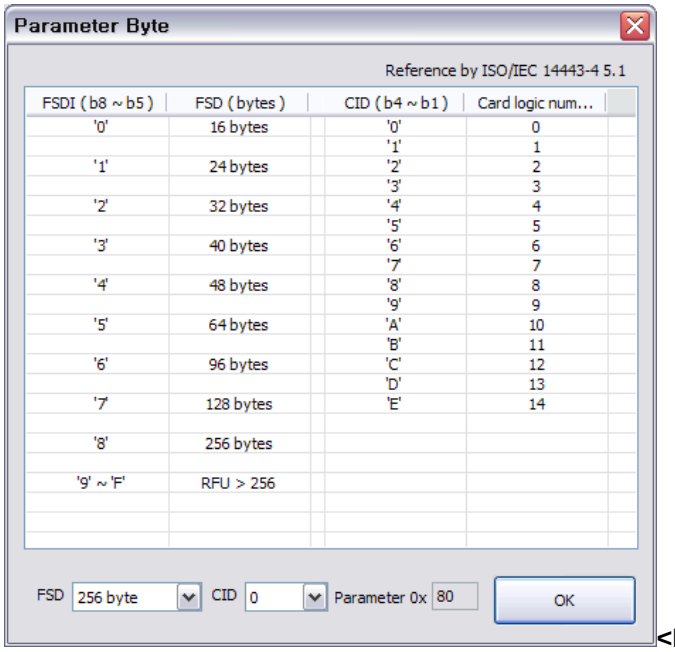



**<Figure 7-2>**

- [REQA]: To execute REQA command.

- [AntiCollision (cascade level)]: To execute Anti Collision (All cascade level) command.

- [RATS]: To execute RATS Command, set parameter from [Parameter 0x 80 ...]. Press [...] to see window for Parameter byte for reference.



**<Figure 7-3>**

- [Analysis]: To analyze response data of RATS command as <Figure 7-3>.

- [Select Application]: To Select Application. Input the application ID at [AID : 000001].

- [Authenticate]: To execute Authentication command.

  Use [Key No 0 KEY 00000000000000000000000000000000] to authenticate.

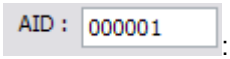
- [Write]: To execute Write command.(**See Example 13.4)**

- [Read]: To execute Read command. (**See Example 13.4)**

- [Credit] : To execute Credit command (reload/recharge/top-up balance).

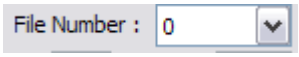
- [Debit] : To execute Debit command (deduct)

- <Figure 7-2> ①

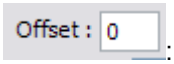


: Set the application ID

-<Figure 7-2> ②



: Select file number (0~16)

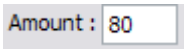


: Set the location to write or read the data from the file

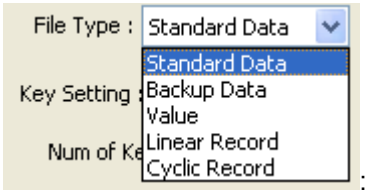
Ex) Offset : 10

Data : 112233445566

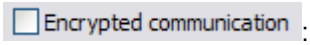
Result of write : 00000000000000000000112233445566000…



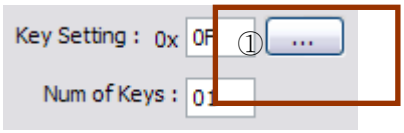
: Set File Size.( In case File Type is Value or Amount value)



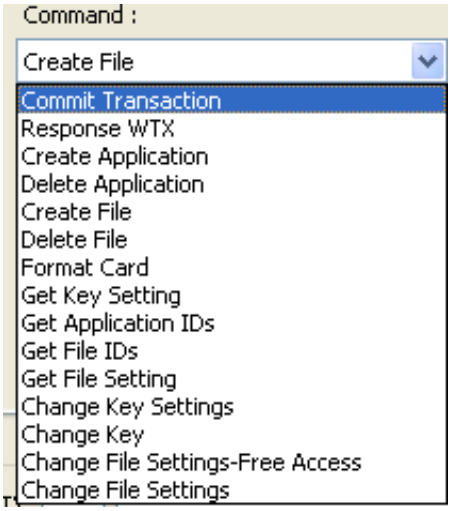
: Select the File



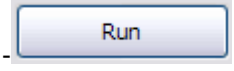
: Check this box in case of using Encrypted communication for write/Read/Credit/Debit Command.



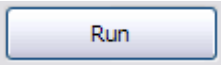

**<Figure 7-4>**



Select the Command to execute from the list

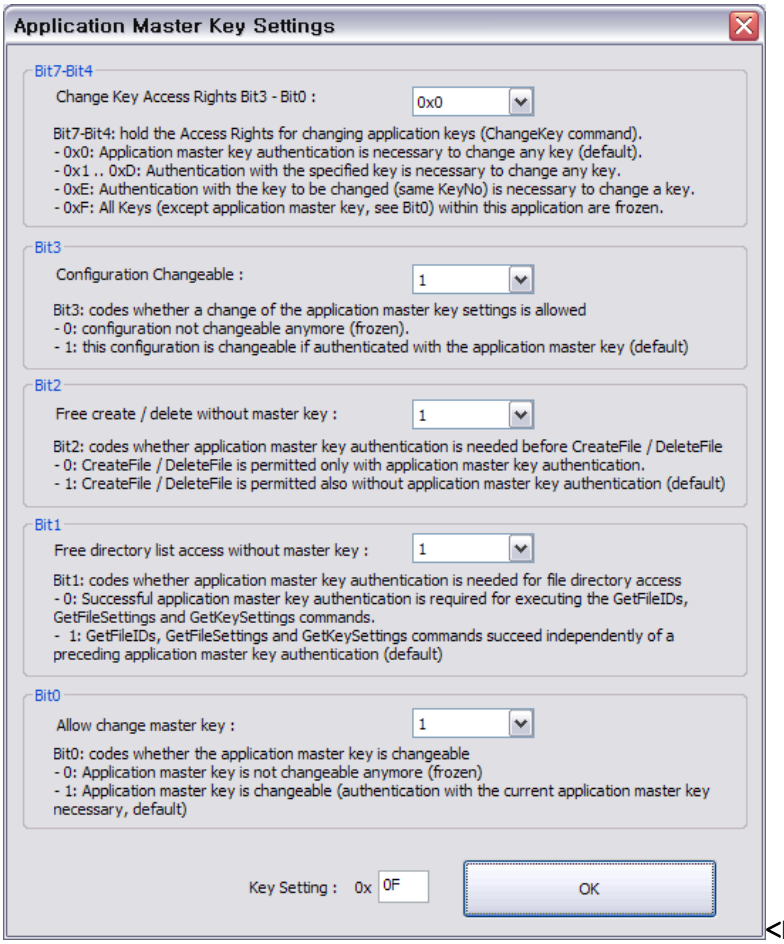
- 

: To execute selected command



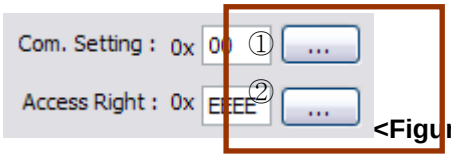

**[Key Setting] :**

It is able to change Key setting value for ‘ Create Application’, ‘Get Key Setting’ and ‘Change Key Setting’ command. Click <Figure 7-4> ① , <Figure 7-5>window will pop up


Application Master Key Settings
Bit7-Bit4
Change Key Access Rights Bit3 - Bit0 :
0x0
Bit7-Bit4: hold the Access Rights for changing application keys (ChangeKey command).
- 0x0: Application master key authentication is necessary to change any key (default).
- 0x1 .. 0xD: Authentication with the specified key is necessary to change any key.
- 0xE: Authentication with the key to be changed (same KeyNo) is necessary to change a key.
- 0xF: All Keys (except application master key, see Bit0) within this application are frozen.
Bit3
Configuration Changeable :
1
Bit3: codes whether a change of the application master key settings is allowed
- 0: configuration not changeable anymore (frozen).
- 1: this configuration is changeable if authenticated with the application master key (default)
Bit2
Free create / delete without master key :
1
Bit2: codes whether application master key authentication is needed before CreateFile / DeleteFile
- 0: CreateFile / DeleteFile is permitted only with application master key authentication.
- 1: CreateFile / DeleteFile is permitted also without application master key authentication (default)
Bit1
Free directory list access without master key :
1
Bit1: codes whether application master key authentication is needed for file directory access
- 0: Successful application master key authentication is required for executing the GetFileIDs, GetFileSettings and GetKeySettings commands.
- 1: GetFileIDs, GetFileSettings and GetKeySettings commands succeed independently of a preceding application master key authentication (default)
Bit0
Allow change master key :
1
Bit0: codes whether the application master key is changeable
- 0: Application master key is not changeable anymore (frozen)
- 1: Application master key is changeable (authentication with the current application master key necessary, default)
Key Setting : 0x 0F
OK

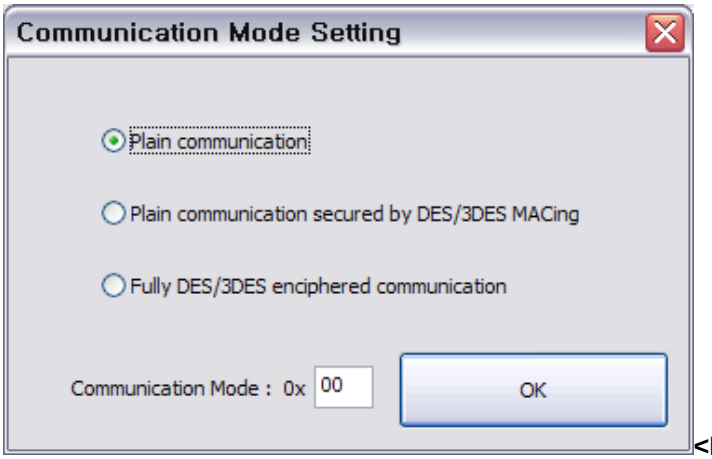
**<Figure 7-5>**

In case selecting following command- Create file, Get file, Change file, Setting-Free Access, Change file setting, <Figure 7-4> would change to <Figure 7-6>.




**<Figure 7-6>**

- Click <Figure 7-6>① , <Figure 7-7> Communication Mode Setting window would pop up. Select one ‘Com. Setting’ value will be changed.



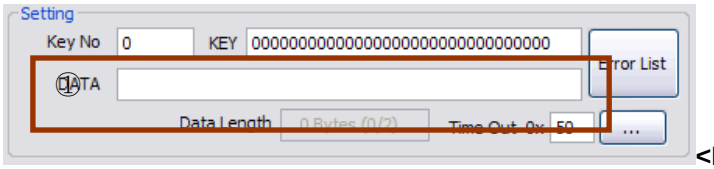

**<Figure 7-7>**

Click <Figure 7-6> ②, Figure<7-8> will pop up, and it is able to change Access rights

Access Rights Setting
Change AccessRights
Access Key No. : Free Access
Read&Write Access (GetValue, Debit, LimitedCredit, Credit for Value files)
Access Key No. : Free Access
Write Access (GetValue, Debit, LimitedCredit for Value files)
Access Key No. : Free Access
Read Access (GetValue, Debit for Value files)
Access Key No. : Free Access
Access Rights : 0x EEEE
OK

**<Figure 7-8>**

**- [Setting]**

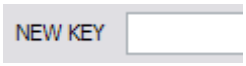



**<Figure 7-9>**

- Key No 0 : Set the 'Key number'.

- KEY 00000000000000000000000000000000 : Show the 'Key value'.

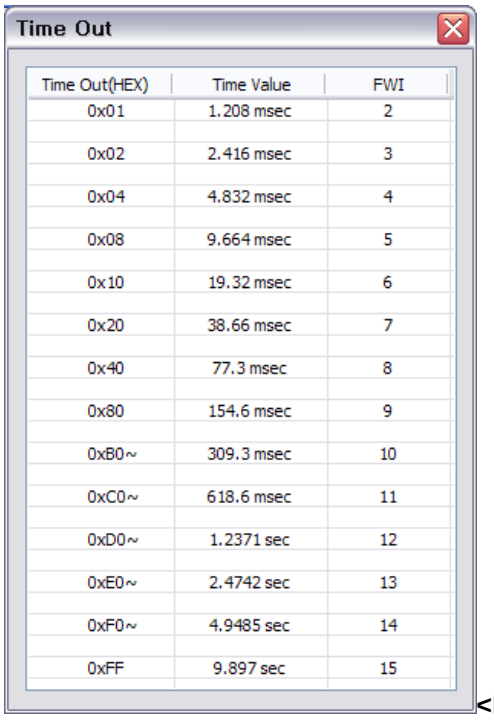
<Figure7-9>① DATA : Input Data.

If you select ‘Change Key’ command, <Figure 7-9>①Data will change to 


-

: You can change ‘Time Out’ Value.

: This button is to show window of reference value of ‘Time out <Figure 7-10>’.

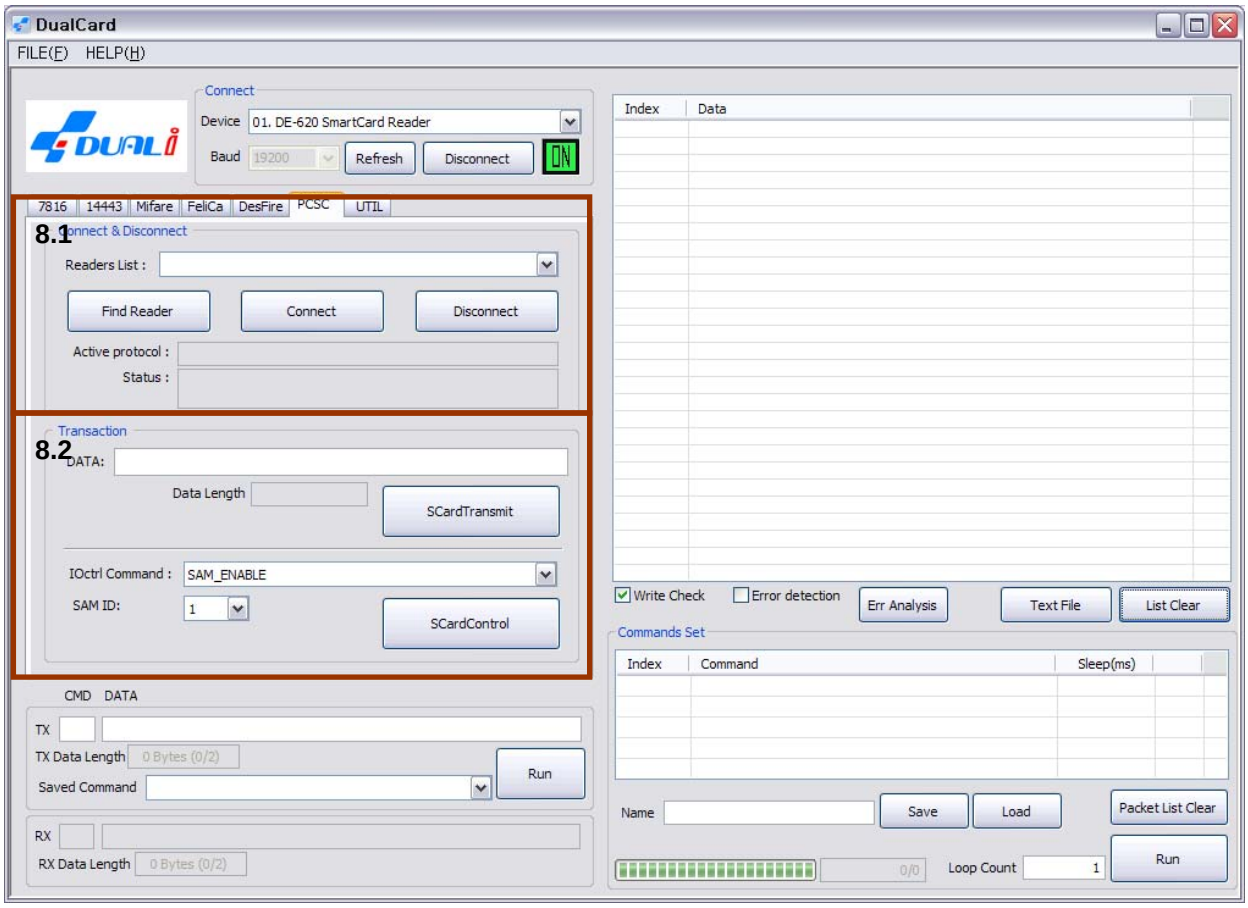


**<Figure 7-10>**

# 8. PCSC

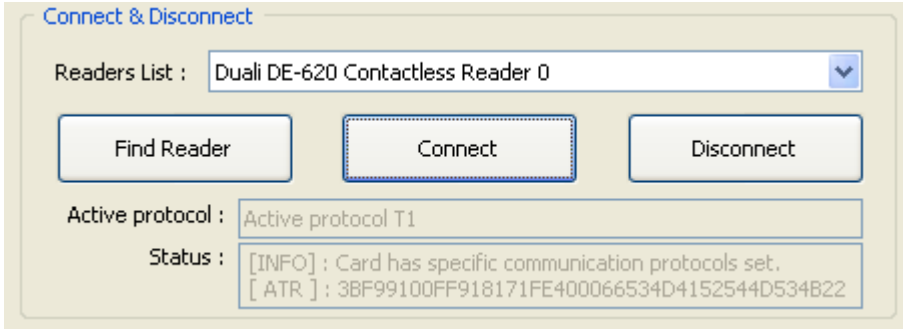
**This tap <Figure 8-1>supports Communication Standard by Microsoft Window, PCSC.**

**This mode works only the connected device supports PCSC mode**

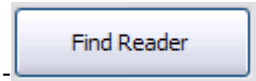



**<Figure 8-1>**

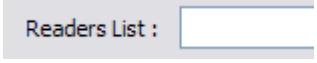
## 8.1 Connect & Disconnect

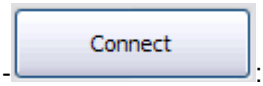



**<Figure 8 -2>**

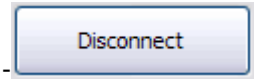



-: To find the PCSC device which is connected to PC, and the device list will be shown



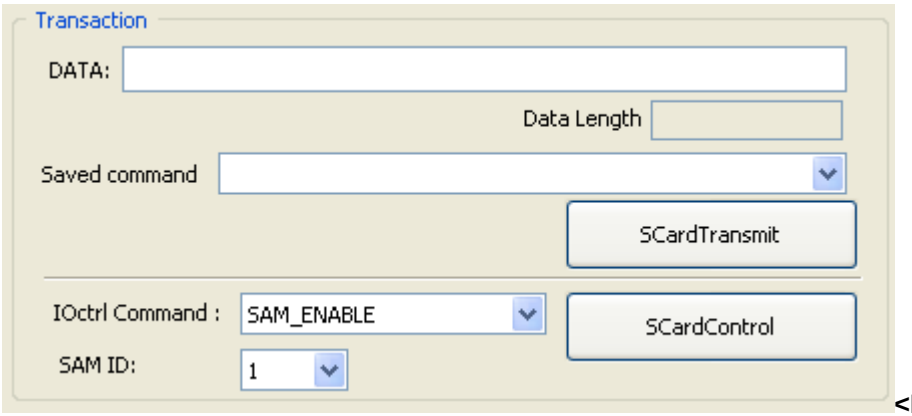


: Select the device and click this button. When card is placed on the device, it'll show the ATR value to the list as a sign of good connection.

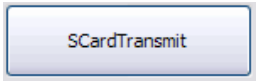


: Disconnect the PCSC device.

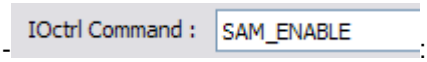
## 8.2 Transaction



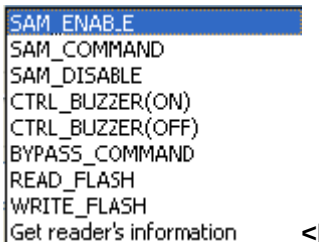
**<Figure 8-3>**

: To Input the command directly. Click 

to execute the data or command

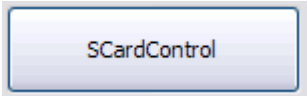


: To use IOctrl Command from PCSC communication spec.



**<Figure 8-4> IOctrl Command list**

: Select the SAM in case device has more than 2 SAM.

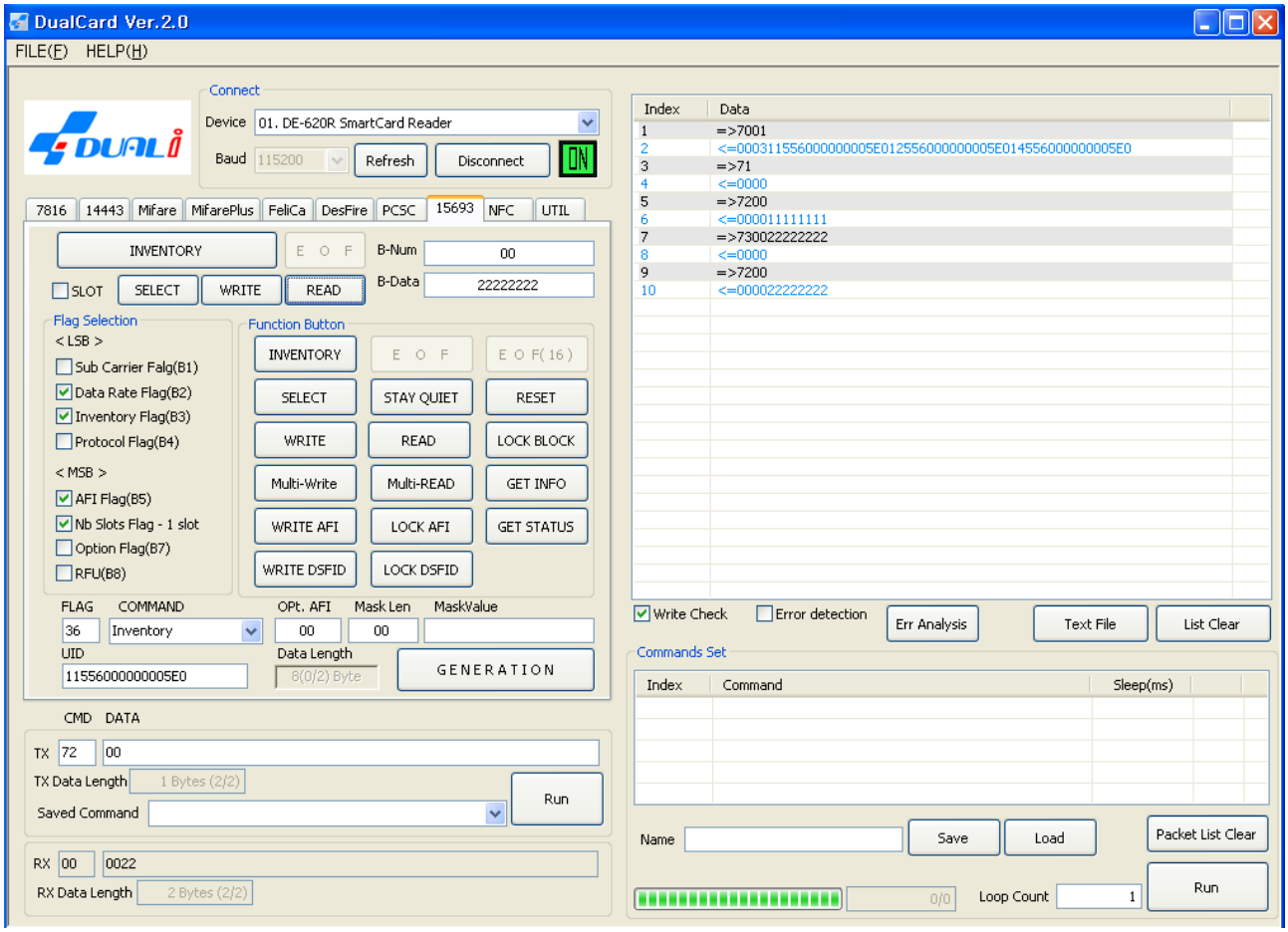


: To execute IOctrl Command.

# 9. 15693 (Optional – DE-620R)

**This tap <Figure 9-1>supports Communication with ISO 15693. NXP's i-Code, Infineon's my-d cards are following ISO Standards.**

**Refer to ISO 15693 or ISO 18000-3 Specification for detail technical information.**




**<Figure 9-1>**

## 9.1 Inventory & Select

: To execute inventory command which defined ISO 15693, and shows Multiple card's information within RF field after Anti-collision process. It shows number of responded card's and each card's UID.

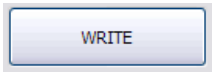
: To Select the last detected card from the multiple cards after Inventory command.

## 9.2 Read / Write

-

: To execute READ command. Input block number to read at

before click READ button. Reading data will be displayed at


- 

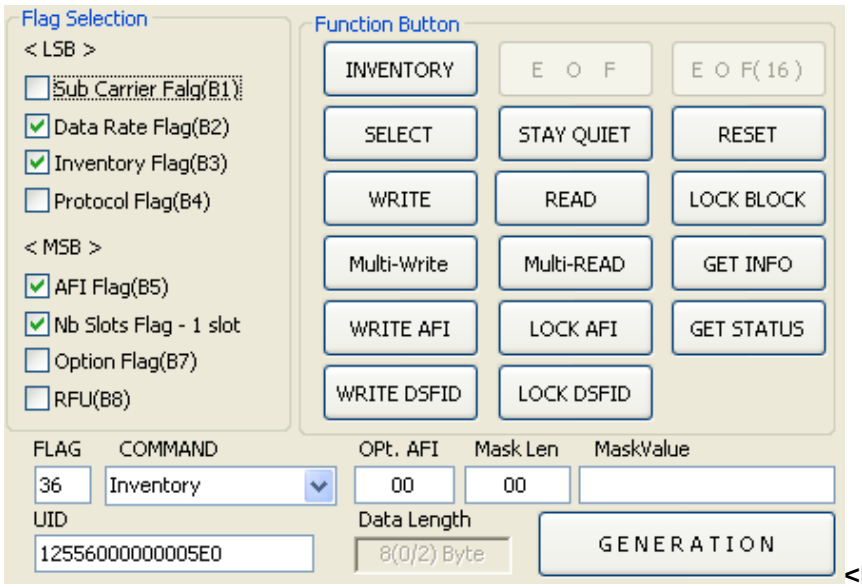
: To execute WRITE command. Input block number to write

and input 4byte data to write at

. before click WRITE button

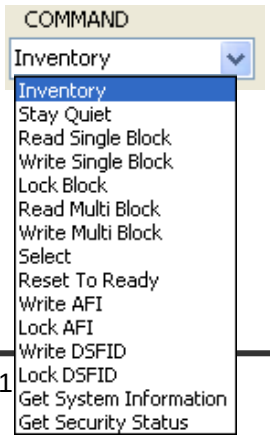
.

## 9.3 Flag Selection, Create Command and Execution



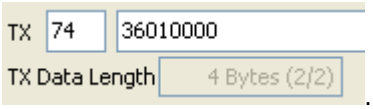
**<Figure 9-2>**

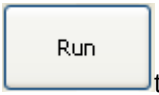
- "Flag Selection" Group box allows User to set flag when Device sending command to Card. Selected flag value is displayed at

.
- "Function Button" have commands set which defined ISO15693 standard, there're also command list at 

to select command

- For each command, different parameter setting window will be displayed.
- Click

button after setting. The command frame will be shown at 

. Click 

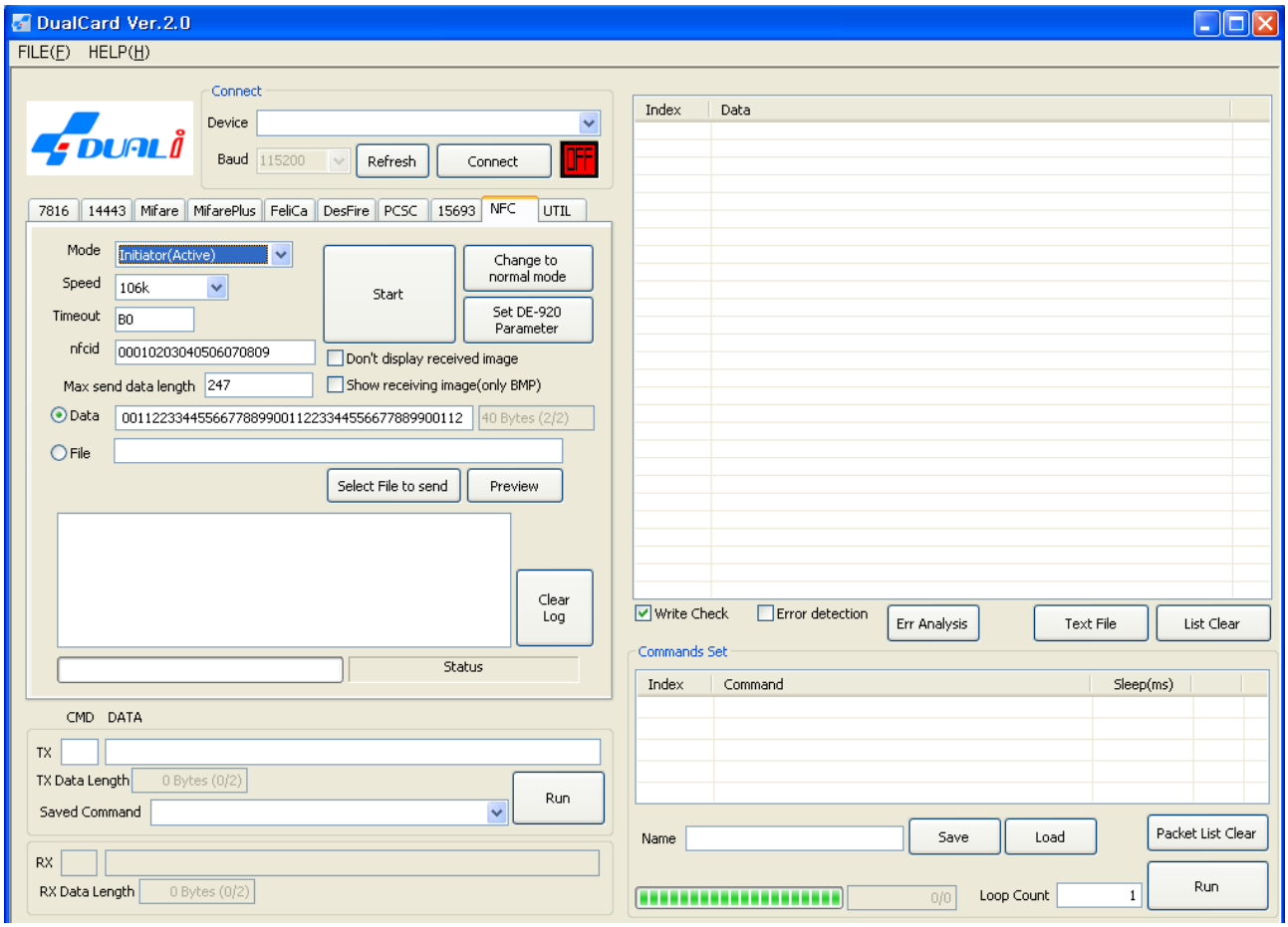
to execute.

# 10. NFC

**This tap <Figure 10-1>supports Communication with ISO 18092( Near Field Communication). ISO 18092 supports communication between Device to Device / Device to Card. Currently the communication speed supports 106/212/424kbps. On speed 106kbps, communication format is similar as ISO 14443 type A. On speed 212/424kbps, communication format is similar as FeliCa.**

**- Passive Communication: Communication between Initiator (create RF field) and Target (receives power from Initiator).**

**- Active Communication: Communication devices both can create RF Field. The one which starts communicate become Initiator. And the other one become Target.**

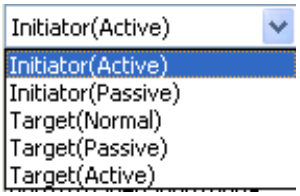


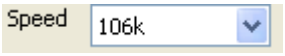

**<Figure 10-1>**

## 10.1 Set Communication Mode

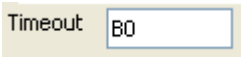
-

: Select Communication mode from the list. There are 5 different modes, Initiator means device which start communication, and Target means device which response to Initiator's command. In Target(Normal) mode, target device set the mode automatically following Initiator's mode.

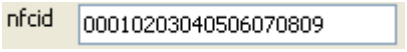



- 

: Set communication speed between Initiator and Target. It supports 106k/212k/424kbps.

- 

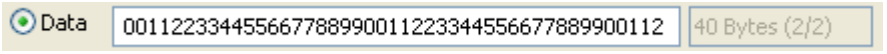
: Set waiting time from sending command and get response.

- 

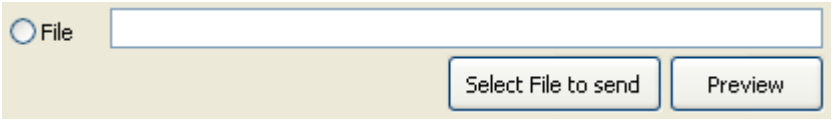
: Random number using for RF Anti-collision of Active & Passive mode. And it also uses SDD(Single Device Detection) process.

-

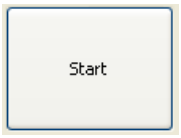
: Max data length of transmission.

- 

: Input Data to send.

- 

: Select File to send.

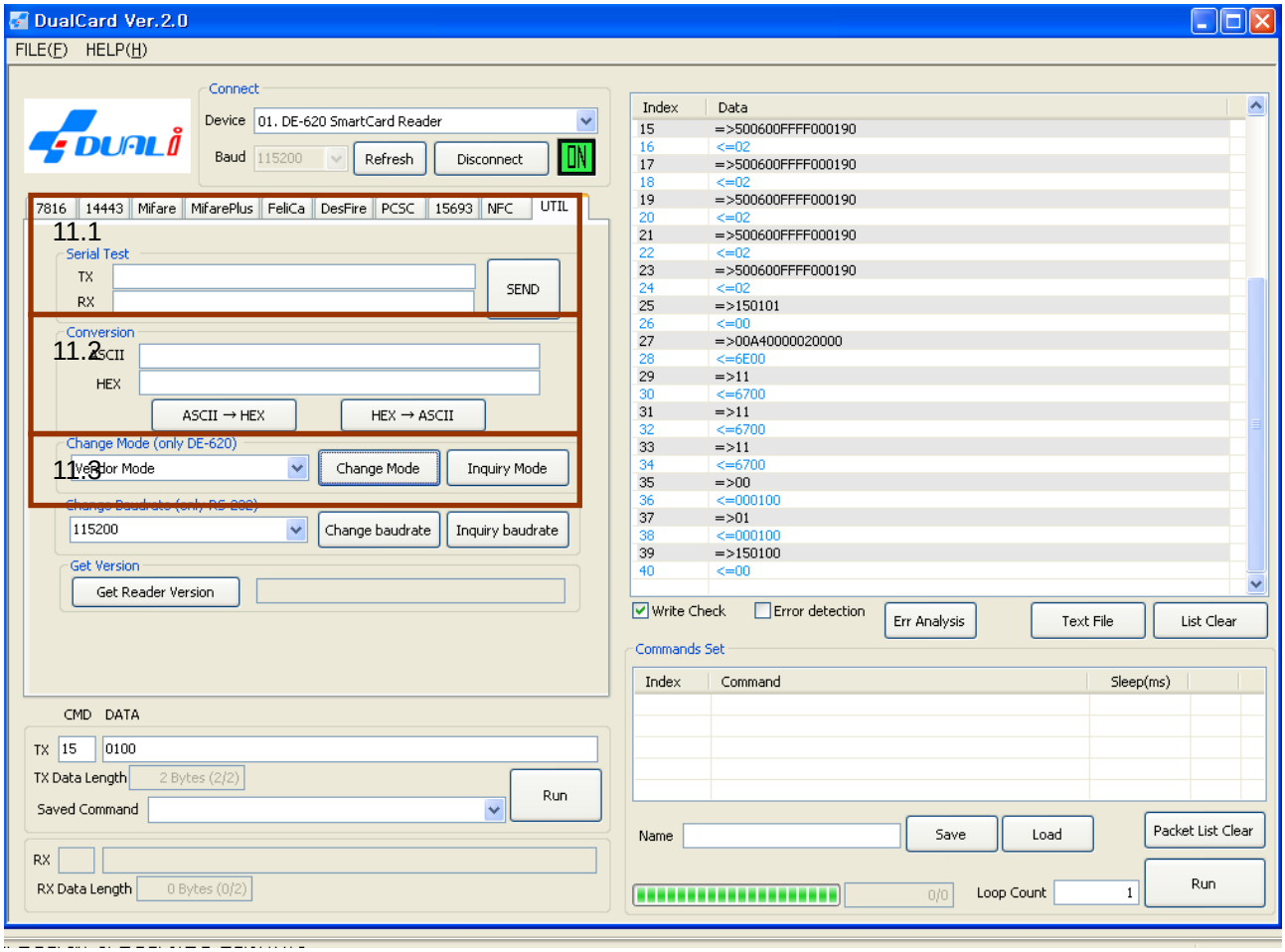
- 

To start communication between two devices. Click this button to start Initiator sending Data/Command.

- **Execute 2 DualCard program and connect two devices. Click Start button from Target first, and Initiator's Start button immediately.**

# 11. UTIL

**This tap <Figure 11-1> is various functions and utility for User's Convenience of using DUALi's devices & software.**




**<Figure 11-1>**

## 11.1 Serial Communication Test

Test of Sending / receiving data In case of using UART. The input data will transfer directly (not using DUALi protocol). It allows DualCard to use UART communication program as well,

-

:To send Input data

-

: Input the Command/ data to send

-

: Response data from the serial equipment is displayed.

## 11.2 Conversion

Convert from ASCII value to HEX value or from HEX value to ASCII value.

-

: Input the ASCII value.

-

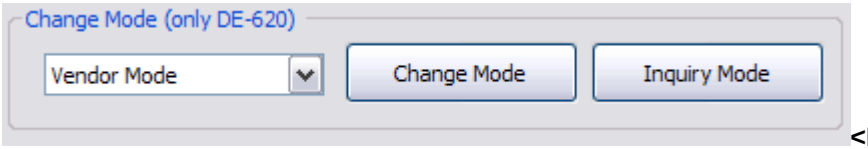
: Input the HEX value.

-

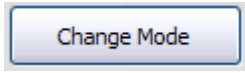
: Convert from ASCII value to HEX value or from HEX value to ASCII value.

## 11.3 Change Mode

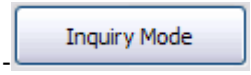
User can easily change from Vendor / PCSC Mode of DUALI devices which support USB.



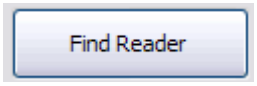
**<Figure 11-2>**

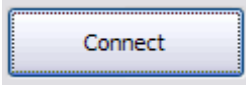
- Select Mode to change and press 


- If PCSC driver is not installed, you have to install driver after you change mode to PCSC mode.

- 

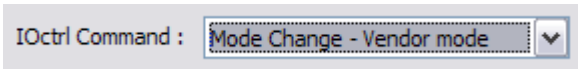
: To check current mode of connected device

- If your OS is Windows7, you should use PCSC tab for changing from PCSC mode to Vendor mode.
  - Click PCSC tab
  - Find PCSC reader using 

button.
  - Click 

button after you select contactless PCSC reader.

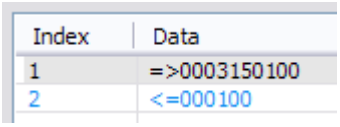
  - Select Change mode like below



- Click

button.

- If you can see log list like below, your device mode is changed.



| Index | Data |
|---|---|
| 1 | =>0003150100 |
| 2 | <=000100 |

# 12. Annex

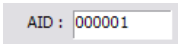
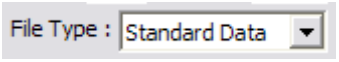
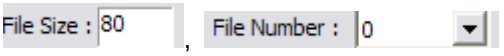
## 12.1 Mifare command

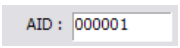
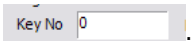
| Command | Explanation |
|---|---|
| Auto Read | Read card Automatically |
| Auto write | Write card Automatically |
| Decrement Transfer | Decrement the value and transfer to selected block |
| Decrement Transfer verify by Reader | Decrement to transfer and verify by Reader. |
| Increment Transfer | Increment to transfer. |
| Increment Transfer verify by Reader | Increment to transfer and verify by Reader. |
| Loadkey | Load Key data to Reader |
| Request Auth | Request, Anticollision, Select, Authentication with KEY No |
| Request Authkey | Request, Anticollision, Select, Authentication with KEY ffffffffffff |
| Request to Read with Key No | Request to Read with KEY No |
| Request to Read with KeyData | Request to Read with KEY ffffffffffff |
| Request to Select | Request to Select. |
| Request to write with key No | Request to write with KEY No |
| Request to write with KeyData | Request to write with KEY ffffffffffff |
| Write for Mifare Ultra Light | Write command for Mifare Ultra Light |
| Req All | Request All command |
| Req Idle | Request Idle command |
| Write Read Verify by App | Write and Read Mifare and Verify by Application |
| Write Read Verify by Reader | Write and Read Mifare and Verify by Reader |

## 12.2 Felica command

| Command | Explanation |
|---|---|
| Polling | Get a value of IDm and PMm |
| Polling-No Auth with RC-251 | Get a value of IDm and PMm without RC-251 Auth |
| Mutual | Authentication command for traditional method |
| Read Block with ENC | Read command for a encrypted Service |
| Write Block with ENC | Write command for a encrypted Service |
| Read Block without ENC | Read command for a non-encrypted Service |
| Write Block without ENC | Write command for a non-encrypted Service |
| Read Block without ENC(Token) | Read command for a non-encrypted Service(Token) |
| Write Block without ENC(Token) | Write command for a non-encrypted Service(Token) |
| Encrement with ENC | Encrement command for a encrypted Service |
| Decrement with ENC | Decrement command for a encrypted Service |
| Cashback without ENC | Cashback command with non-encrypted Service |
| Read Balance | Read Balance |

## 12.3 DesFire command

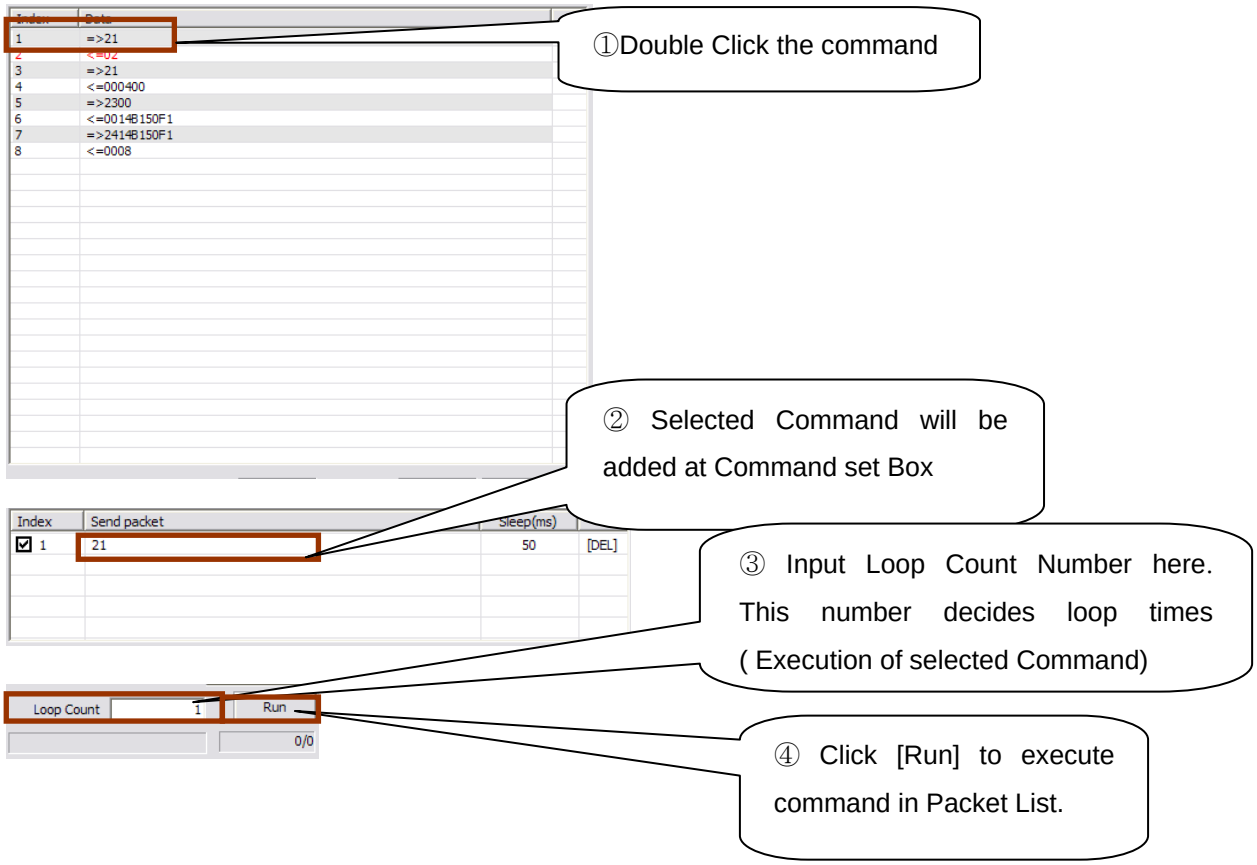
| Command | Explanation |
|---|---|
| Commit Transaction | This command allows to validate all previous write access on Backup Data Files, Value Files and Record Files within one application. |
| Response WTX | If the PICC needs more time than the defined FWT to respond to a PCD command it will send a request for a waiting time extension. |
| Create Application | This command allows to create new applications on the PICC.<br>You need to set  to Create Application |
| Delete Application | This command allows to permanently deactivate applications on the PICC. |
| Create File | This command create files according to selected file type  . (Standard Data, Backup Data, Value, Linear Record, Cyclic Record)<br>You need to set  |
| Delete File | This command permanently deactivates a file within the file directory of the currently selected application. |
| Format Card | This command releases the PICC user memory. |
| Get Key Setting | This command allows to get information on the PICC and application master key settings. In addition it returns the maximum number of keys which can be stored within the selected application. |
| Get Application IDs | This command returns the Application IDentifiers of all active applications on a PICC. |
| Get File IDs | This command returns the File IDentifiers of all active files within the currently selected application. |
| Get File Setting | This command allows to get information on the properties of a specific file. The information provided by this command |

| | |
|---|---|
| | depends on the type of the file which is queried. |
| Change Key Settings | This command changes the master key settings depending on the currently selected AID.<br>  |
| Change Key | This command allows to change any key stored on the PICC.<br>You need to input Key No in  . |
| Change File Settings-Free Access | This command changes the access parameters of an existing file for free access |
| Change File Settings | This command changes the access parameters of an existing file. |

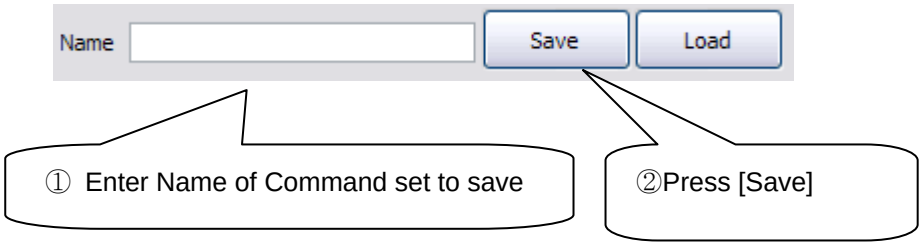
# 13. Example

## 13.1 Add command to packet list and Save/Load command set

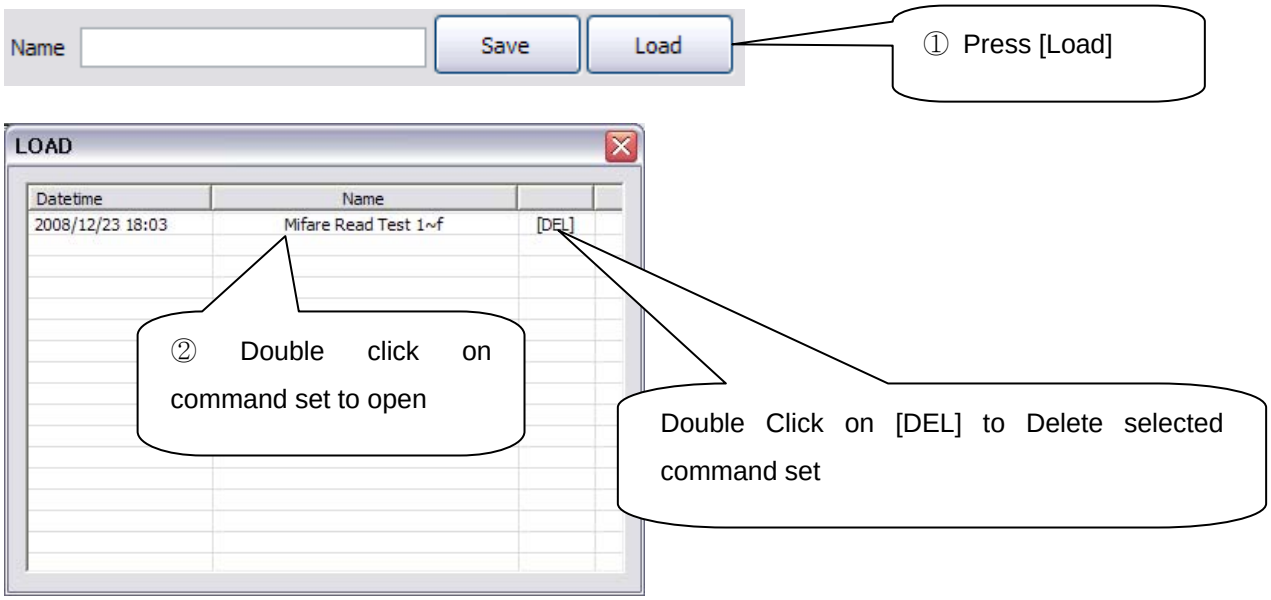
*** Add command to Packet List :**




*** Save Command set**

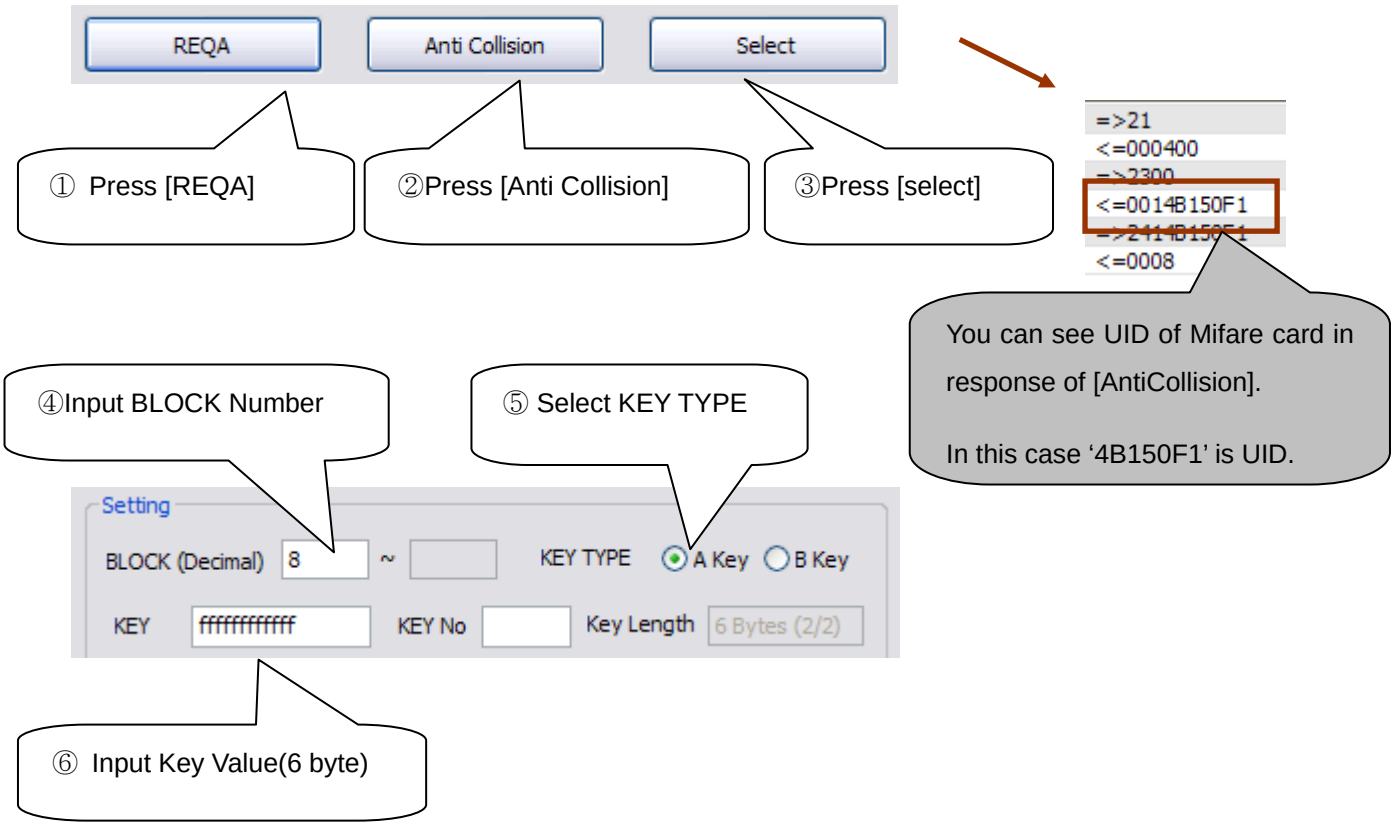


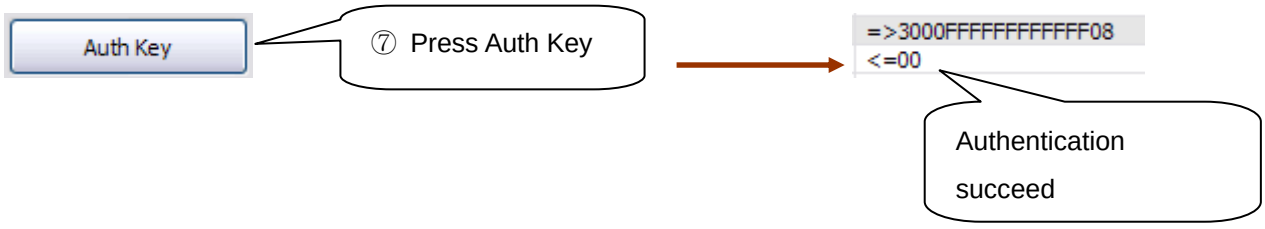
*** Load/Delete Command set**



## 13.2 Mifare

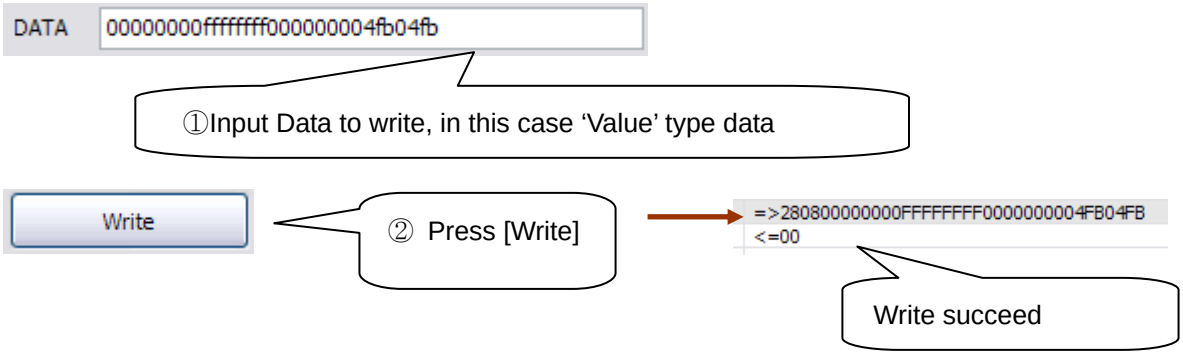
*** [Auth Key] Authentication**



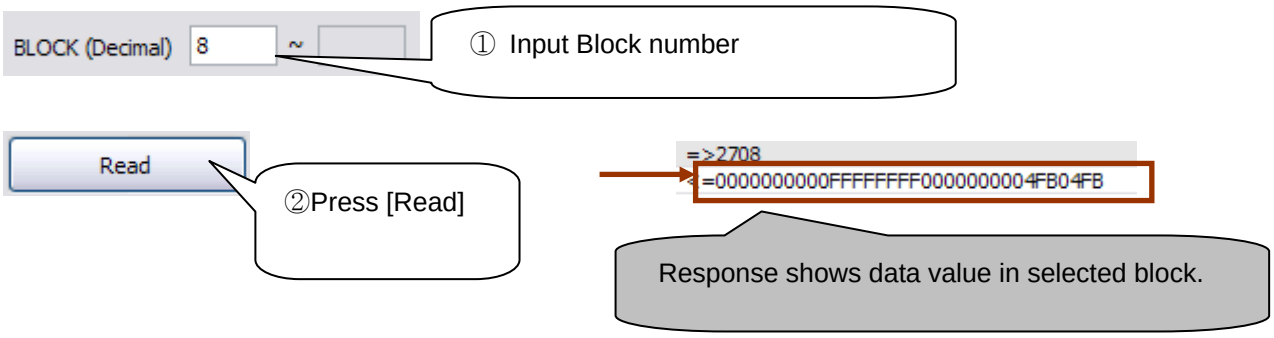

*** [Write]**

Write process has to made after [Auth Key] Procedure



*** [Read]**

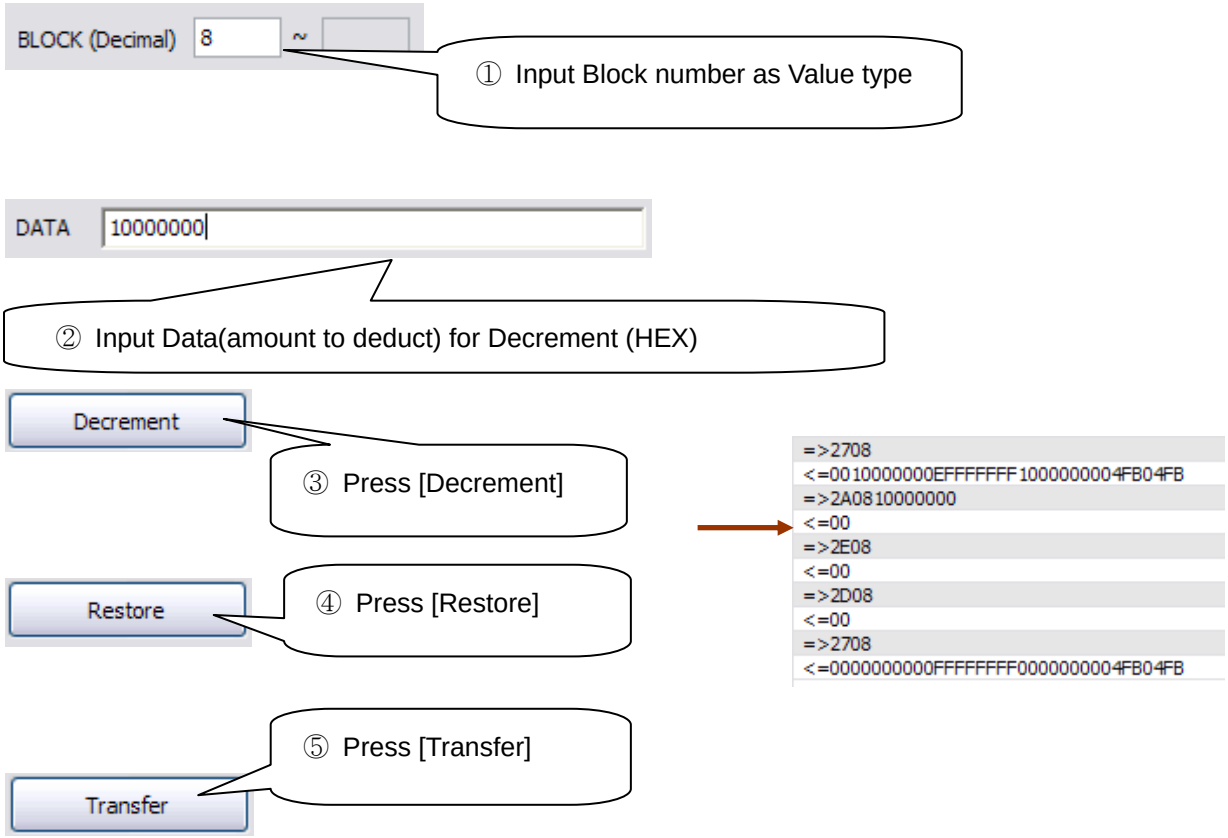
Read process has to made after [Auth Key] Procedure




*** [Decrement]**

Decrement process has to made after [Auth Key] Procedure

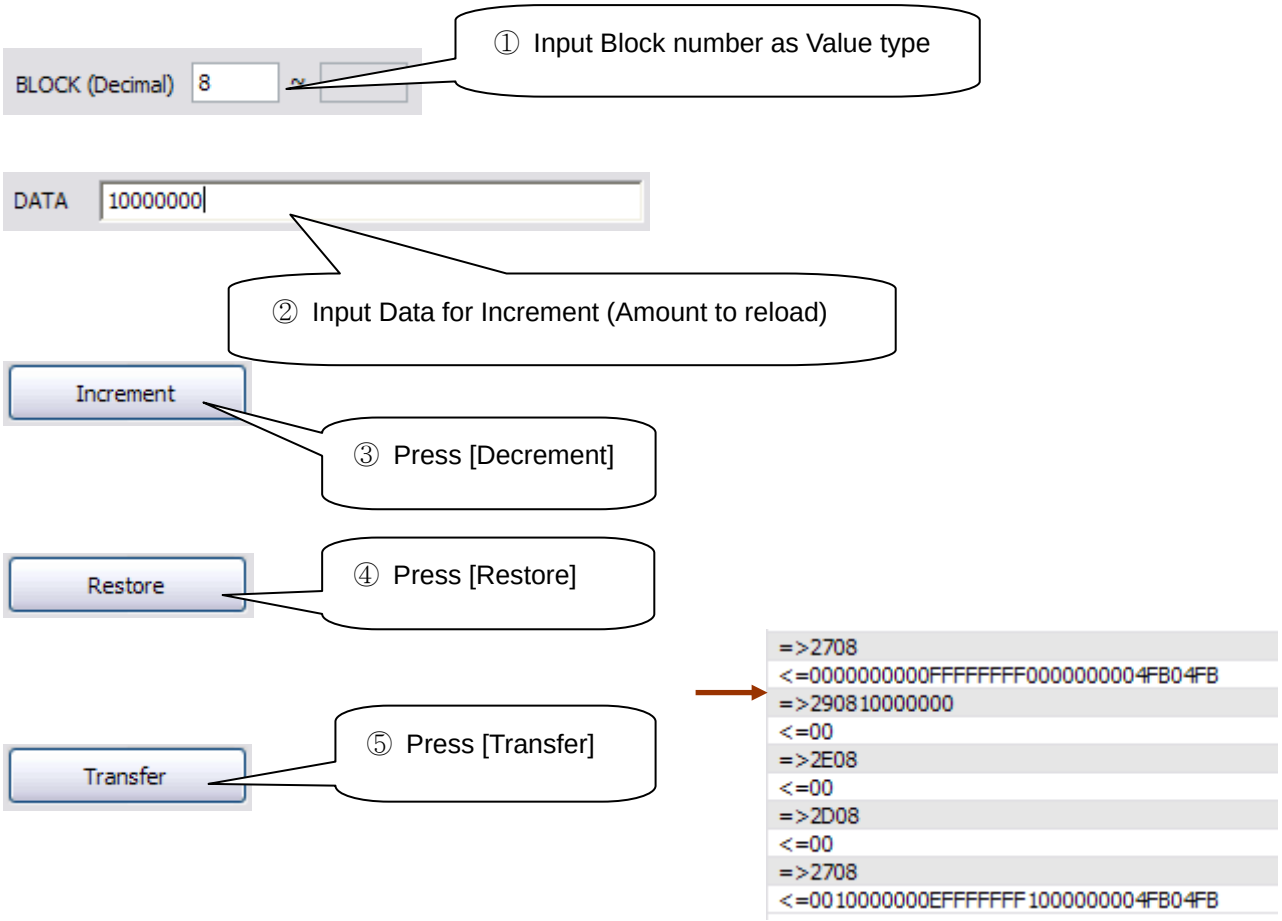
For Decrement, block data must be 'Value type'.



*** [Increment]**

Increment process has to made after [Auth Key] Procedure

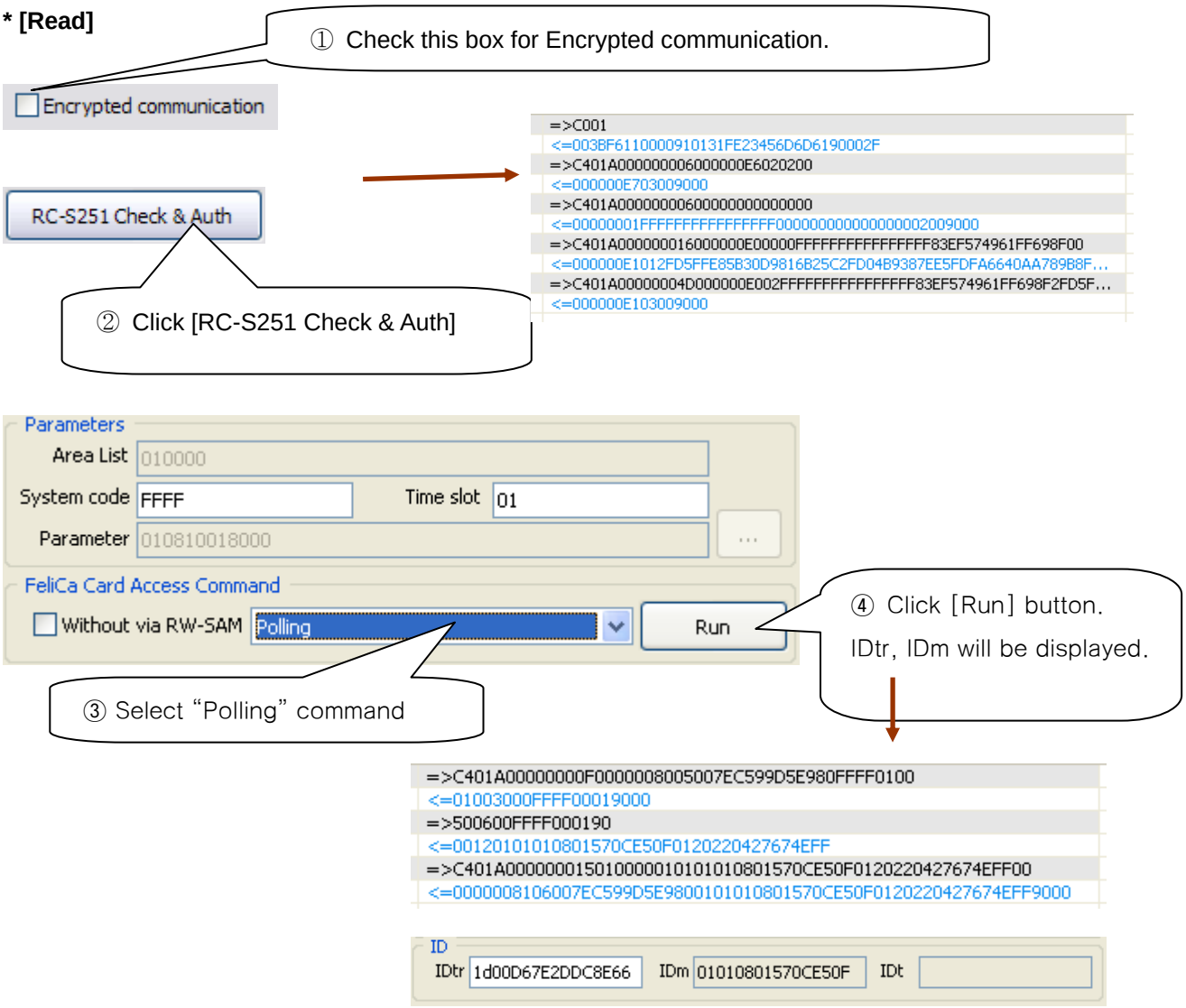
For Increment, block data must be ‘Value type’.



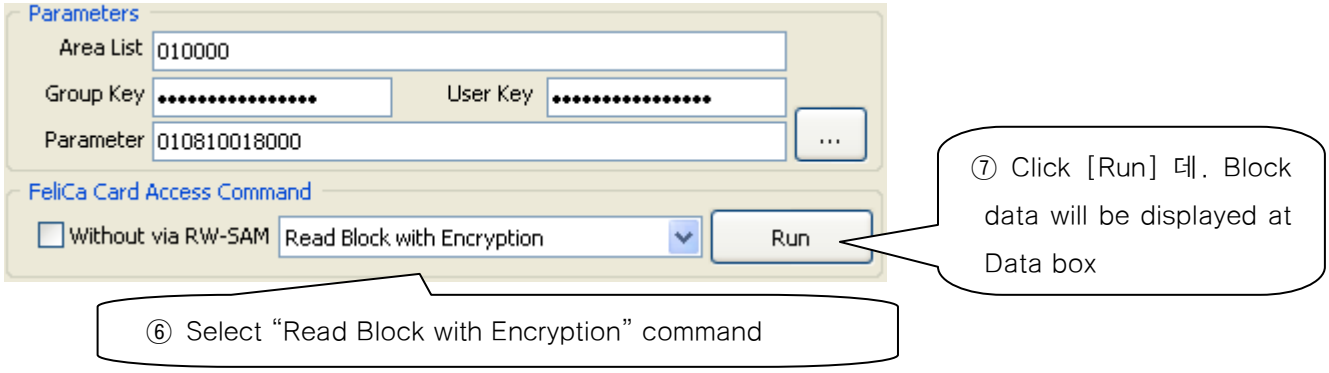
## 13.3 Felica

- This procedure based on FeliCa SAMPLE5 card.

*** [Read]**

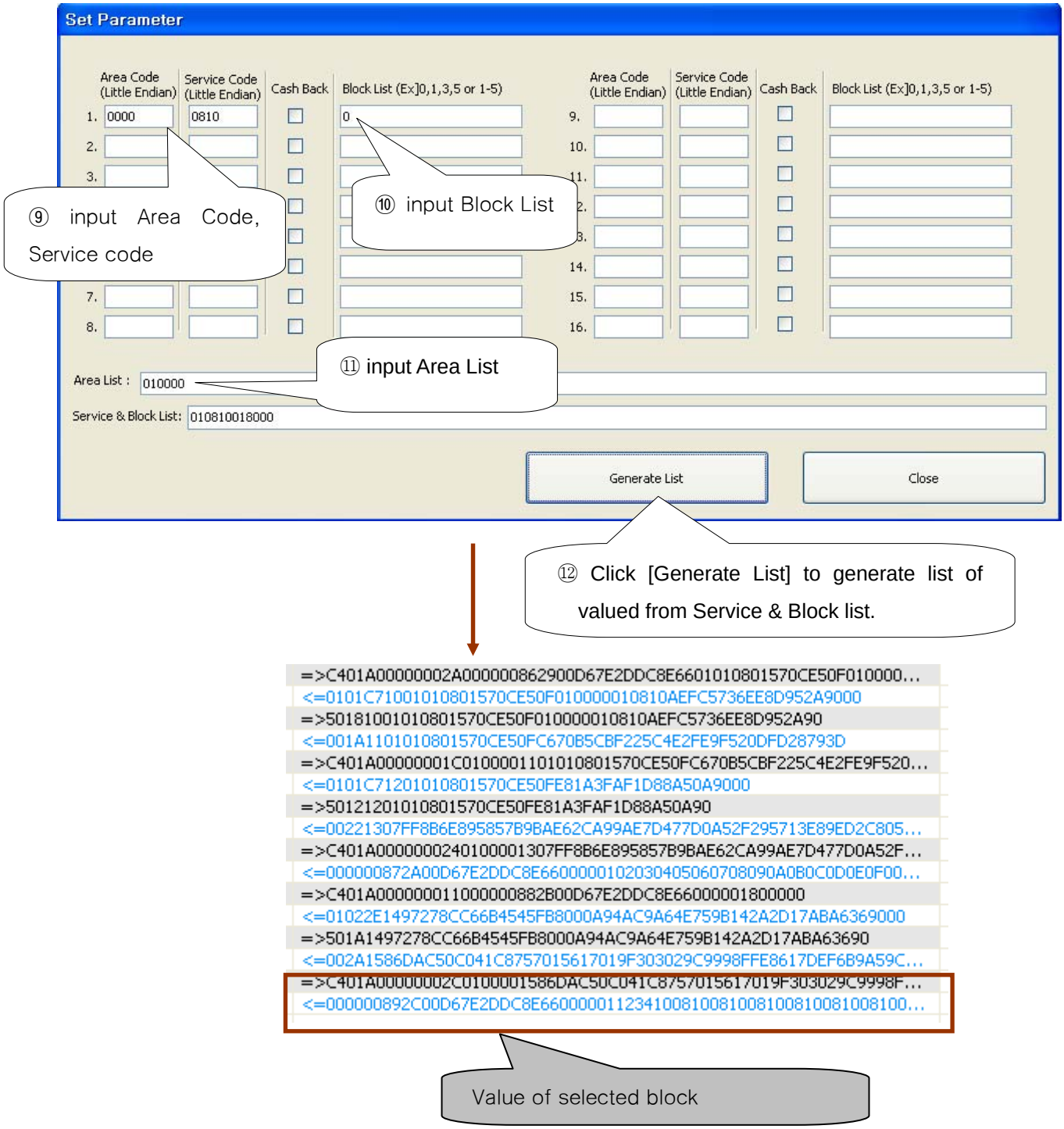



⑤ Default key for Sample 5 card is set which needs for Read command.



⑧ To set parameter except commands from the list, click

, following "Set Parameter" window will pop up.



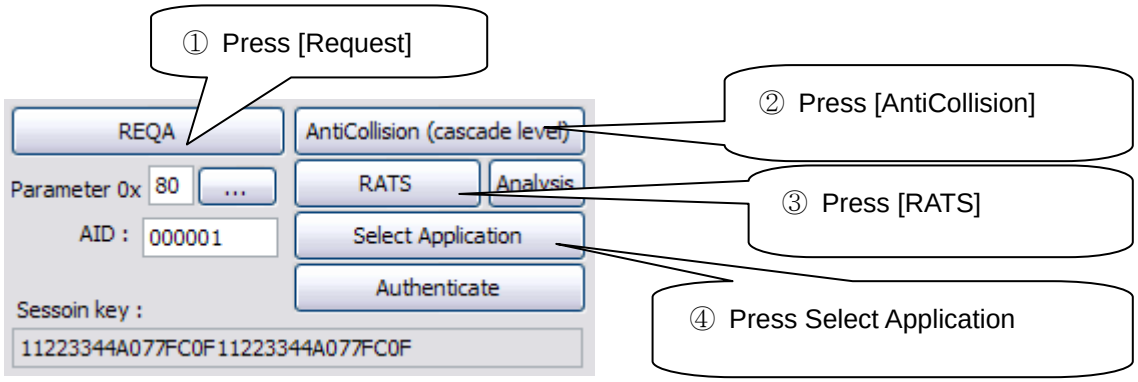
* [Write]

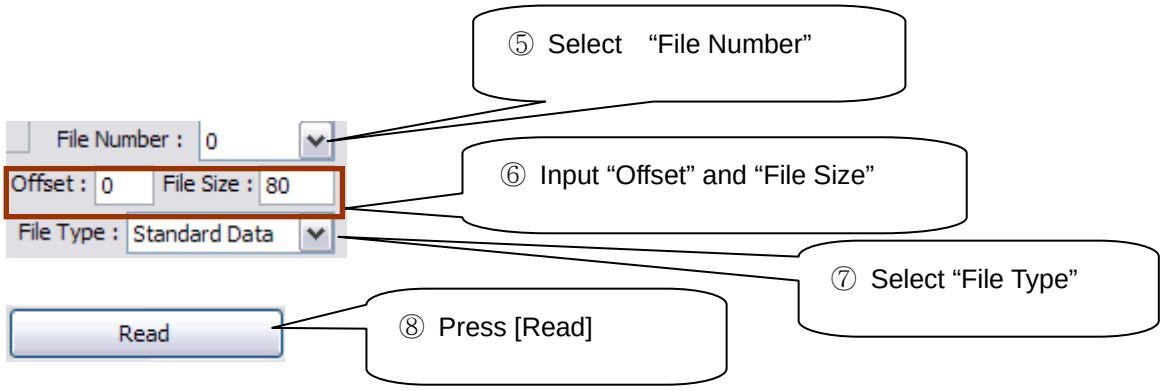
RW-SAM Authentication process is required before Write process.(same as Read)

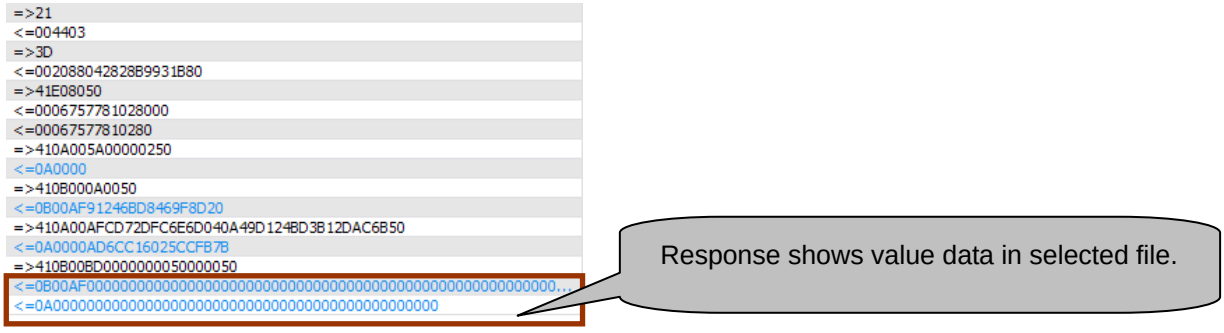
## 13.4 DesFire

- This procedure based on default key value and standard data file type.
- AID is '000001'

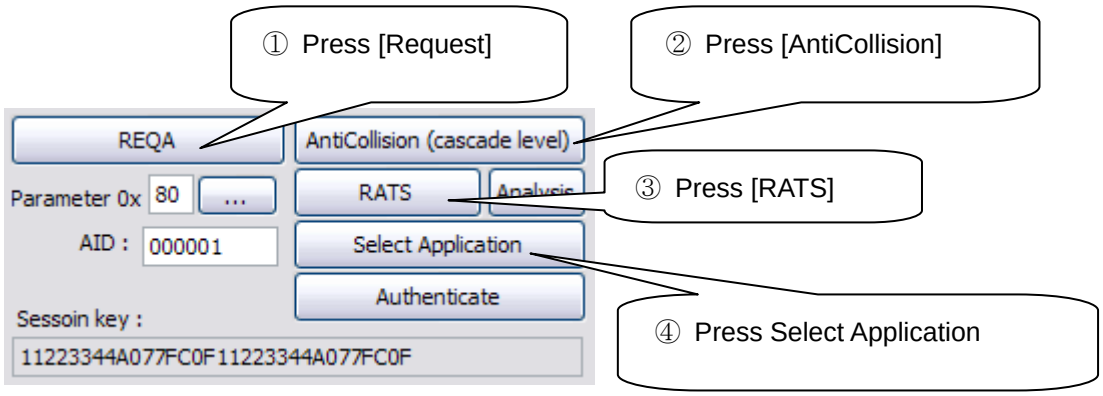
*** [Read]**

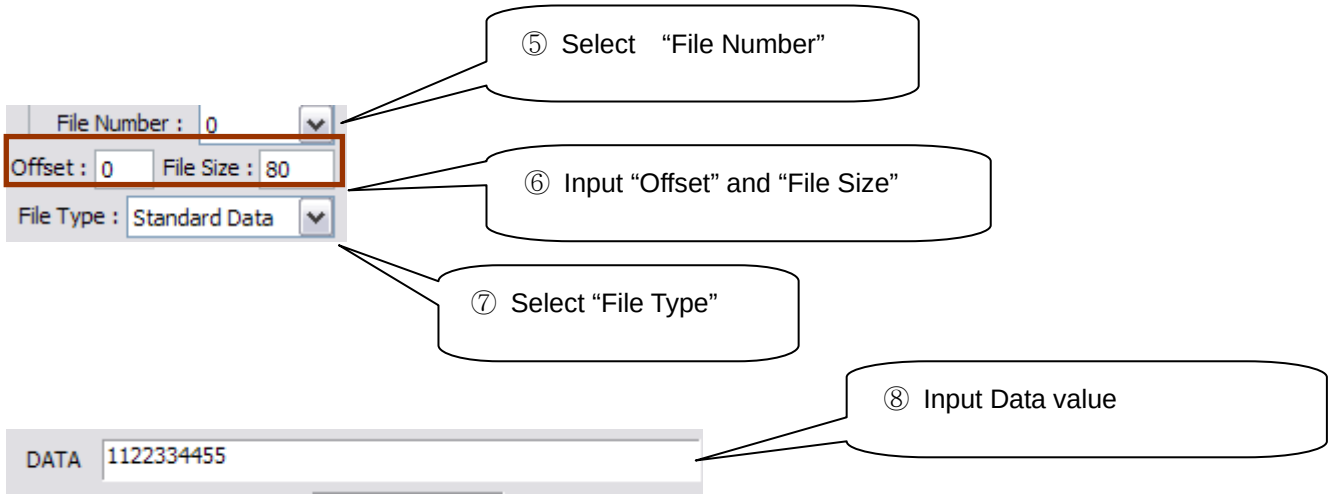


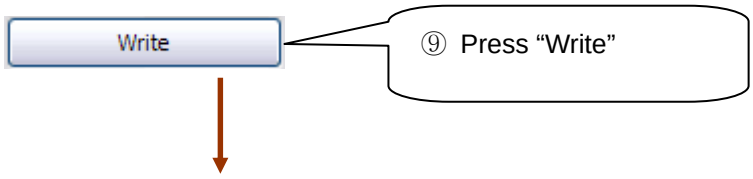



*** [Write]**



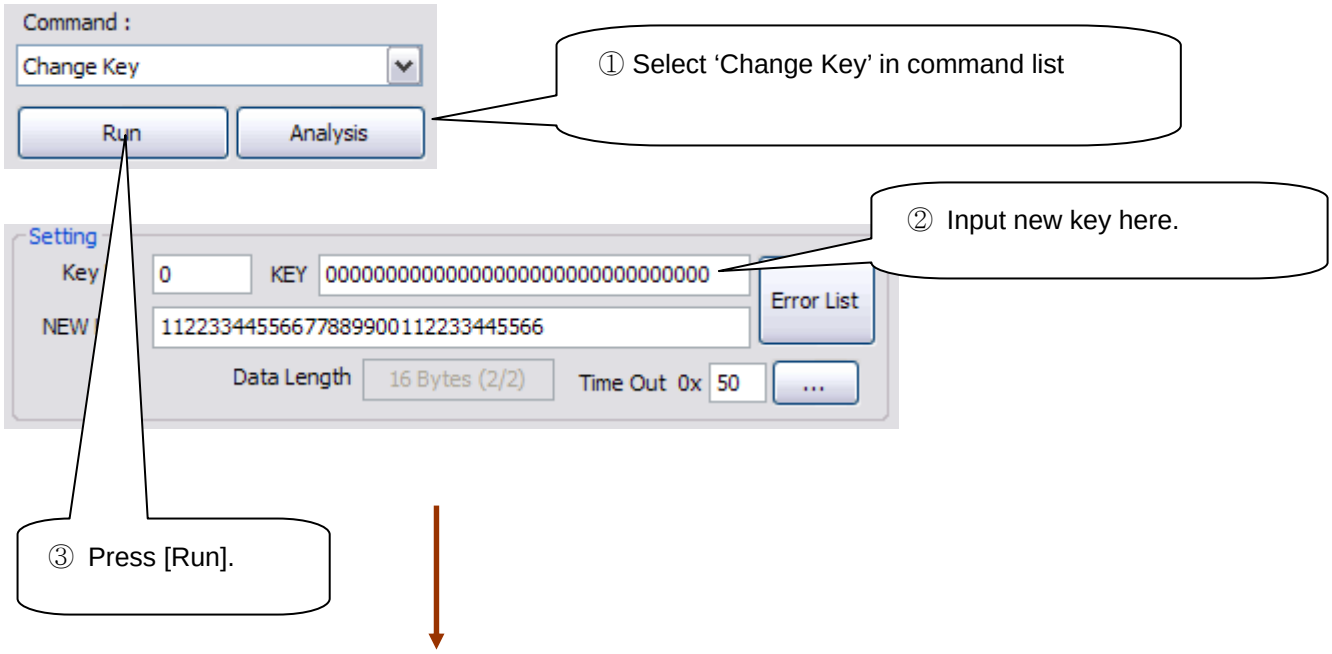




```
=>410B003D0000000005000011223344555O
<=0B0000
=>410A00BD0000000050000050
<=0A00AF1122334455000000000000000000000000000000000000000000000000...
<=0B0000000000000000000000000000000000000000000000000000
```

*** [Change Master Key]**

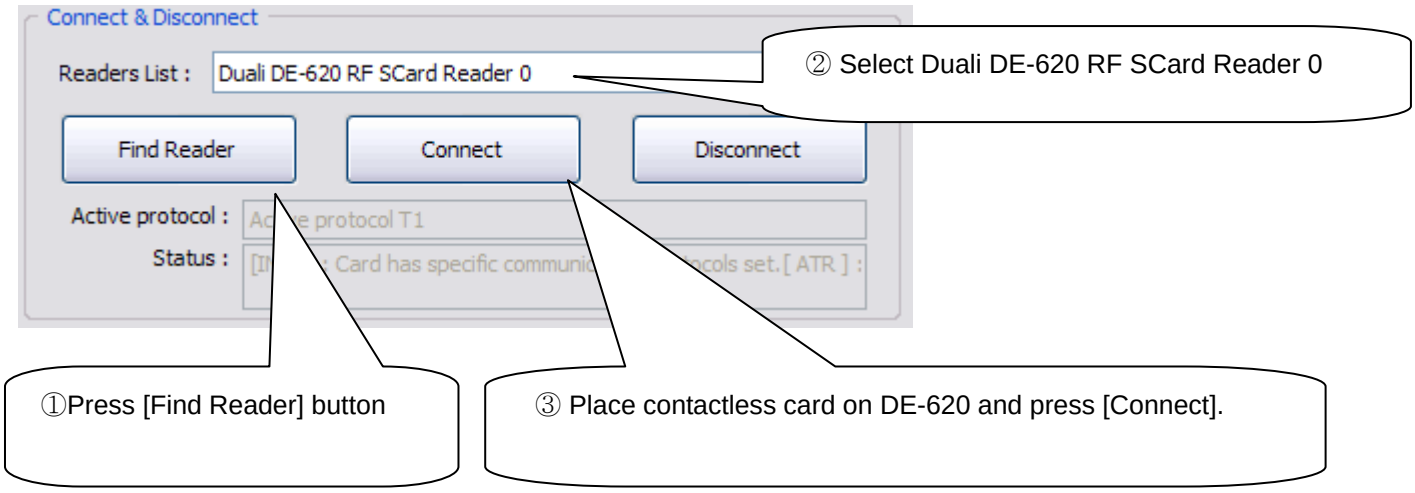
Key ‘0’ Authentication process is required before this process.

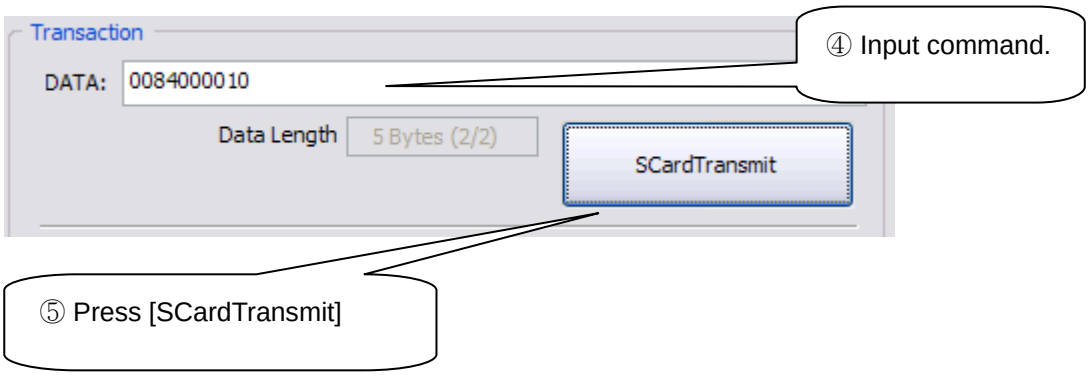



```
=>410A00AFCD72DFC6E6D040A43BD1E221EB51D9F950
<=0A0000AD6CC16025CCFB7B
=>410B00C400981D76D84D746B536E7AE64787E500E9AE821207ABF8231150
<=0B0000
```

## 13.5 PCSC

This explanation is for using PCSC mode of connected DUALi device




- SCardControl